

Minnesota Department of Human Services Aging and Adult Services Division

Request for Proposals for Additional PHR Community Collaboratives to Demonstrate Personal Health Records for Beneficiaries of Long Term Services and Supports

Date of Publication: July 18, 2016

Americans with Disabilities Act (ADA) Statement: This information is available in accessible formats for people with disabilities by calling 651-431-2600 or by using your preferred relay service. For other information on disability rights and protections, contact the agency's Americans with Disabilities Act (ADA) coordinator.

Contents

I. Introduction	4
A. Purpose of Request	4
B. Objective of this RFP	4
C. Background	4
II. Scope of Work	7
A. Overview	7
B. Tasks and Deliverables	10
III. Proposal Format	15
A. Required Proposal Contents	16
B. Proposal Requirements	17
C. Innovative Concepts (If Applicable)	26
D. Required Statements	27
IV. RFP Process	34
A. Responders' Conference Webinar	34
B. Responders' Questions	34
C. Proposal Submission	35
V. Proposal Evaluation and Selection	36
A. Overview of Evaluation Methodology	36
B. Evaluation Team	36
C. Evaluation Phases	36
D. Contract Negotiations and Unsuccessful Responder Notice	38
VI. Required Contract Terms and Conditions	38
VII. State's Authority	44
Appendix A: Business Requirements Document	46
Appendix B: Detailed Business Requirements Workbook	47
Appendix C: PHR for LTSS Demo – Glossary and Selected Acronyms	48
Appendix D: Resources	54
Appendix E: Responder Commitment to Require Vendor Completion of DHS Vendor Security Questionnaire	56
Appendix F: DHS Vendor Security Questionnaire	57
Appendix G: Sample State Grant Contract	75
Appendix H: Sample Data Sharing and Business Associate Agreement	85

Appendix I: PHR Vendor Review of Requirements Documentation Statement 105

I. Introduction

A. Purpose of Request

The [Minnesota Department of Human Services \(DHS\)](#), through its Aging and Adult Services Division (State), is seeking proposals from qualified responders to:

1. Demonstrate an electronic [Personal Health Record \(PHR\)](#) system for Minnesota beneficiaries of [Long Term Services and Supports \(LTSS\)](#) funded by [Medical Assistance \(MA\)](#) Waivers. Responders are not asked to develop a new, state-wide PHR system, but to demonstrate an enhanced PHR system tailored to beneficiaries of LTSS), as described in detail in this RFP.
2. Participate in pilot execution and evaluation of a nationally developed electronic LTSS (e-LTSS) standard.

The demonstration is funded by a federal [Testing Experience and Functional Tools \(TEFT\)](#) grant from the [Centers for Medicare & Medicaid Services \(CMS\)](#).

B. Objective of this RFP

The objective of this RFP is to contract with up to three qualified responders to perform the tasks and services set forth in this RFP. The State intends to select respondents for up to three contracts ranging between 12 and 18 months, subject to negotiation and available grant funds. The term of the contracts are anticipated to begin between November 1, 2016 and April 1, 2017 (or the date when final contract signatures are obtained) to March 31, 2018 with the option for up to two extensions.

This is the second round of funding offered for this purpose. The State has contracted with the Otter Tail PHR Community Collaborative, which is scheduled to launch the first release of its PHR in Otter Tail County in late 2016. The State has received additional funding from CMS to expand the demonstration to additional communities.

Proposals must be submitted by email by 4:00 p.m. Central Time on Friday, September 2, 2016. This RFP does not obligate the State to award a contract or complete the project, and the State reserves the right to cancel the solicitation if it is considered to be in its best interest. Contract awards are subject to availability of funding from the Centers for Medicare and Medicaid Services (CMS). All costs incurred in responding to this RFP will be borne by the responder.

C. Background

According to the 2013 DHS Report "[Status of Long Term Services and Supports](#)," "Minnesota spent over \$3.6 billion on long-term services and supports in state fiscal year 2012 through Medical Assistance programs. Seventy-five percent (75%) of those expenditures were supporting older adults and people with disabilities through home and community-based services." DHS collects and maintains data about more than 54,000 monthly recipients of Home and Community-Based services from Counties, Tribes, Managed Care Organizations (Lead

Agencies) and LTSS service providers. This data includes annual functional and financial assessments, screening documents, community support plans, coordinated service and support plans, service agreements, case management notes, as well as service encounter and claims data.

Currently, some of this data is shared with the [beneficiaries](#) or their [legal representatives](#) through printed documents delivered by hand or through US Mail. However, there is currently no way for beneficiaries or their legal representatives to access this information electronically. Paper versions of documents can be easily discarded or misplaced. This can make it very difficult for the beneficiary or legal representative to maintain a comprehensive understanding of the MA funded LTSS they are receiving. DHS works to ensure that information provided to beneficiaries/legal representatives is clear and understandable, however the information beneficiaries/legal representatives retain and file may often be difficult to understand and interpret.

The [CMS Fact sheet on Home and Community Based Services](#), “specifies that service planning for participants in Medicaid HCBS programs under section 1915(c) and 1915(i) of the Act must be developed through a [person-centered planning process](#) that addresses health and long-term services and support needs in a manner that reflects individual preferences and goals.” CMS thus requires that Minnesota beneficiaries of MA-funded LTSS must be at the center of input and decision-making in their care planning. Effective person-centered planning requires that the beneficiary has complete information regarding that beneficiary’s care and services. Beneficiaries, their legal representatives, and their families must have access to understandable, relevant information to effectively direct a person-centered planning process. The State believes that making some of the information that it maintains about beneficiaries available to beneficiaries through a secure, online Personal Health Record (PHR) is a vital component to person-centered planning. Information about a beneficiary’s services and supports belongs to that beneficiary, and the State has an obligation to provide it to them in the most accessible, understandable and useable format possible.

LTSS information in a PHR will be available whenever the beneficiary/legal representative signs in without requiring that it be separately retained and filed by the beneficiary or their legal representative. In order to make information available in a PHR, the State will need to create a mechanism to allow its existing systems to interact with evolving external systems based upon industry standards. The State is modernizing its existing systems to comply with the [Medicaid Information Technology Architecture \(MITA\)](#) framework. This modernization requires the State to use standards-based interaction for [Health Information Exchange \(HIE\)](#).

A June 2013 DHS Continuing Care Administration Report, [Expansion of Electronic Health Records for Long Term Services and Supports](#), found that expanding the use of Electronic Health Records (EHR) for LTSS beneficiaries would result in improved care transitions and care coordination, improved data analytics within DHS systems, and would help ensure a person-centered, beneficiary owned approach to data . The State is pursuing ways to use Health

Information Technology (HIT) to further this goal. DHS applied for funding from CMS to demonstrate use of HIT through a PHR in October 2013.

CMS considers Health Information Exchange to be an important goal for State Medicaid agencies. In February of 2016, it issued a letter ([SMD# 16-003](#)) to state Medicaid Directors indicating that “90 percent HITECH match would be available for States’ costs related to the design, development, and implementation of infrastructure for several HIE components and interoperable systems that most directly support Eligible Providers in coordinating care with other Medicaid providers in order to demonstrate Meaningful Use.” Additionally, CMS is considering “pre-certification” of Modular Medicaid IT Enterprise Solutions, according to a recently released [Request for Information \(RFI\)](#).

DHS is one of nine state Medicaid agencies awarded a four-year CMS TEFT Grant in 2014. The State has opted to participate in all four aspects of the CMS TEFT Grant program. The CMS TEFT Grant program requires the State to accomplish the following goals:

1. Demonstrate use of Personal Health Record systems with beneficiaries of [Community-Based Long Term Services and Supports \(CB-LTSS\)](#); and
2. Assist in identifying, evaluating and harmonizing a national standard for electronic Long Term Services and Supports (e-LTSS) data in conjunction with the [Office of the National Coordinator’s \(ONC\) Standards and Interoperability \(S&I\) Framework](#); and
3. Field test a beneficiary experience survey within multiple CB-LTSS programs for validity and reliability; and
4. Field test a modified set of “Functional Assessment Standardized Items” (FASI) functional assessment measures for use with beneficiaries of CB-LTSS programs.

This Request for Proposals will result in funding up to three additional “Minnesota Personal Health Record Community Collaboratives” (Collaborative) which will work closely with the State and Minnesota’s Information Technology Agency (MN.IT@DHS) staff to accomplish the first two goals of the CMS TEFT Grant.

In November of 2015, the State contracted with the Otter Tail PHR Community Collaborative (OTPCC) through the first release of this Request for Proposals. The OTPCC is working closely with [MN.IT@DHS](#) and DHS business staff to demonstrate a PHR solution, with the first release scheduled to launch in early October, 2016. The Collaborative has also done extensive work on an eLTSS Standard, and is testing the exchange of a set of 122 fields of data between members of the OTPCC.

II. Scope of Work

A. Overview

This RFP provides background information and describes the services desired by the State. It delineates the requirements for this procurement and specifies the contractual conditions required by the State. Although this RFP establishes the basis for Responder Proposals, the detailed obligations and additional measures of performance will be defined in the final contract. A selected glossary of terms and acronyms used in this RFP is included as [Appendix C](#).

1. Goals and Outcomes:

The Collaborative will work with MN DHS and MN.IT@DHS staff to:

- a) Develop, test and deploy the required modifications to a PHR system (as described in Section [II.B.1.d](#)) that will allow participating beneficiaries of MA services to access information about their services, enter information about themselves online (e.g., notes, diary entries or other functions that may exist in the PHR system - this does not include making edits to DHS data), and securely share access to that information as they choose with family or others (i.e. health care providers, case managers, LTSS providers, etc.),
- b) Develop and/or administer existing processes and policies to ensure privacy and consent safeguards are in place to comply with the [Health Insurance Portability Accountability Act \(HIPAA\)](#), [Minnesota Health Records Act](#), Title 38 Section 7332 Protections Confidentiality of Certain Medical Records, and [MN Government Data Practices Act \(MDPA\)](#) regulations, and
- c) Participate in testing an e-LTSS data standard within existing Collaborative systems and/or the PHR as required by the ONC S&I process.

2. Available Funding:

The State intends to award up to \$750,000, subject to receipt of Federal grant funds, for up to three Collaboratives as a result of this RFP. Individual contract amounts are subject to negotiation and availability of Federal grant funds and may range from \$250,000 to \$750,000. There is no requirement that any Collaborative or entity match these funds. However, applicants will need to describe in-kind funding and its sources in their project budget.

3. Grant Timeline:

Event	Date Due
RFP posted on State Register	Monday, July 18 , 2016
RFP Responders' Conference Webinar	Monday, August 8, 2016, 2:00 p.m. – 3:30 p.m. CDT or in person in Room 2390 of the Elmer L. Anderson Building in St. Paul, MN
All questions due to DHS in writing (Note: after this date no more questions will be addressed by DHS)	Monday, August 15, 2016, 4:00 p.m. CDT
Responses to written questions posted on PHR for LTSS Demo web page	Friday, August 19, 2016, 4:00 p.m. CDT
Proposals due to DHS	Friday, September 2 2016, 4:00 pm CDT
Anticipated proposal review period	Monday, September 5 – Friday, September 23, 2016
Anticipated notice of intent to award	Friday, September 23, 2016
Anticipated negotiation period	Monday, September 23 – Monday, October 31, 2016
Desired contract execution	Between Tuesday, November 1, 2016 and Friday, December 30, 2016
Contract end date	Friday, March 30, 2018

4. Eligible Applicants:

Respondents to this RFP must be the single entity that will serve as the representative of its proposed Community Collaborative. Single organizations without other committed partners are not eligible for this grant.

The Community Collaborative must meet the following minimum criteria:

- a) Consist of two or more organizations participating in assessment, care provision, case management or payment administration of MA-funded Long-Term Services and Supports for Minnesotans.
- b) Have at least one member who has a current contract with the MN Department of Human Services (DHS) to serve as an Integrated Health Partnership (IHP); or who is otherwise part of an Accountable Care Organization (ACO) in Minnesota. To be considered participating in an ACO, the responder must be participating in Medicare ACO demonstration like Pioneer, MSSP, or Next Generation; or Responder must have a cost of care contract with a health plan in Minnesota.
- c) Have a lead partner that will serve as the applicant organization for the grant. The applicant organization must meet the State's fiscal requirements and other grant

participation requirements, including the ability to collect and submit data and manage staffing, facilities, communication, and other grant operations. The State will fund the successful proposed Community Collaborative through a grant contract with the lead partner. The lead partner will be contractually responsible for ensuring that the Community Collaborative accomplishes the goals, tasks and deliverables set forth in this RFP.

- d) Have a community-led leadership team that represents the community and all participating providers.
- e) Serve a limited, definable geographic area.
- f) The Community Collaborative should include partners that serve Minnesotans receiving services paid for by Medical Assistance. This list is representative of the types of partners that may be part of the Collaborative. The Collaborative must include at least one Skilled Nursing Facility (SNF) and at least one Home and Community-Based Services provider but does not have to include *all* of these partner types:
 - i. Home and Community-Based Services (HCBS):
 - A. Assisted living facilities
 - B. Home health organizations
 - C. Social services or social supports
 - D. Community health boards/local health departments
 - E. LTSS providers
 - ii. County, Managed Care Organization (MCO), or Tribe (also referred to as “Lead Agencies” in Minnesota) and their case managers. NOTE: this is not the same as the “lead partner” listed above. “Lead Agency” is a State designation for a County, MCO or Tribe. “Lead partner” is the member of the Collaborative that will serve as the contracting agency with the State on the part of the Collaborative. The “lead partner” for the Collaborative may or may not be a “Lead Agency”.
 - iii. Acute care:
 - A. Hospitals
 - iv. Post-acute care:
 - A. Skilled Nursing Facilities
 - v. Primary care:
 - A. Primary care clinics
 - B. Community clinics
 - C. Rural Health Clinics
 - D. Federally Qualified Health Centers
 - E. Health care homes
 - F. Specialty clinics
 - G. Behavioral health clinics/facilities
- g) Serve a minimum of 50 percent of MA beneficiaries in their limited, definable geographic area with LTSS.
- h) Have in place (or agree to develop within the first half of the grant period):

- i. Data sharing agreements and consent management protocols established between all partners and beneficiaries/guardians as needed, in adherence with all applicable laws,
 - ii. A contract with a MN certified [Health Information Exchange Service Provider \(HIESP\)](#), and
 - iii. Functioning electronic health record (EHR) system(s) certified by the Office of the National Coordinator for [Health Information Technology Certification Program](#) or [MN state “Qualified” EHR](#) in use by one or more Collaborative member.
- i) Provide letters of commitment from each member which describes their role(s) and commitment to participate in the leadership team and the overall PHR Demonstration project.

B. Tasks and Deliverables

1. Tasks:

- a) Develop and manage a PHR Community Collaborative (as described in the “Eligible Respondents” section above):
- i. Provide or develop a suitable governance structure,
 - ii. Facilitate meetings and coordinate the Collaborative and necessary operational resources,
 - iii. Participate in regular meetings with the State and MN.IT@DHS staff throughout the course of the project to ensure successful integration of State “back end” functionality with the public-facing PHR and to ensure that users of the PHR have sufficient input and support to maximize the effectiveness of the system,
 - iv. Provide project management of the PHR Community Collaborative grant, including maintenance of work plans, regular meetings with State project leadership, etc.,
 - v. Prepare and submit regular progress and financial reports to MN DHS as directed,
 - vi. Participate in State and federal evaluation of the demonstration, including a “Lessons Learned” process that will be conducted by the State at the end of the demonstration,
 - vii. Participate as requested by the State in presentations to relevant groups such as the [MN Age and Disabilities Odyssey](#) and the [MN e-Health Summit](#) about lessons learned from the demonstration.
- b) Identify needs and requirements of the beneficiaries or legal representatives that will use the PHR.
- c) Identify needs and requirements of the Collaborative.
- d) Develop, test and deploy the necessary modifications to a Personal Health Record system for beneficiaries of MA services.
- i. The Collaborative may choose from one of the following options for obtaining a Personal Health Record system:

- A. One or more members has an existing contract with a vendor of an electronic health record (EHR) system certified by the Office of the National Coordinator for [Health Information Technology Certification Program](#) or [MN state "Qualified" EHR](#) with PHR functionality which could be modified and used for this project, or
- B. The Collaborative or one or more members of the Collaborative has an existing contract with a [Minnesota State-Certified Health Information Exchange Service Provider \(HIESP\)](#) which has PHR functionality which could be modified and used for this project, or
- C. The Collaborative will establish a contract with a vendor of a PHR product which can be modified and used for this project. If the Collaborative chooses this option, selection of the PHR vendor is subject to approval by the State.
 - ii. In collaboration with the State, develop, test and deploy the required modifications to a secure, web-based Personal Health Record (PHR) system to ensure that it meets the requirements set forth in the Business Requirements Document ([Appendix A](#)) and Detailed Business Requirements Spreadsheets ([Appendix B](#) - available to download as a separate MS Excel document from the [PHR for LTSS Demo web page](#)) in this RFP. The Collaborative's contracted PHR technology provider must indicate in writing that it has thoroughly reviewed the requirements documentation, is willing to participate in the project, and that its technology solution is capable of meeting the RFP requirements (with exceptions noted in the Detailed Business Requirements Workbook). The form included as [Appendix I](#) must be signed by the vendor's authorized representative and submitted as part of the Collaborative's response to the RFP.
 - iii. Work closely with DHS and MN.IT @ DHS staff to ensure secure, accurate, timely integration of data from DHS systems into the PHR as described in the attached requirements documentation.
- e) Develop and/or administer processes and policies to ensure privacy and consent safeguards are in place for the PHR to comply with the [Health Insurance Portability Accountability Act \(HIPAA\)](#), [Minnesota Health Records Act](#), Title 38 Section 7332 Protections Confidentiality of Certain Medical Records and [MN Government Data Practices Act](#) regulations. Process and policy documents must meet the criteria in section [II.B.2.c](#) of this RFP.
- f) Participate in the DHS Security Lifecycle Management process.
- g) Require that the Collaborative's contracted PHR vendor(s) complete the "MN Department of Human Services Vendor Security Questionnaire" (a sample is provided in [Appendix F](#)) as required by the State.
- h) Ensure that all required security practices are followed throughout the course of the contract.
- i) Recruit LTSS beneficiaries and legal representatives served by Collaborative members, as well as caregivers, lead agency case managers, providers and other relevant users to participate in focus groups, usability testing, beta testing and use of the PHR in production. The successful respondent will work with State staff and/or consultants to

ensure that beneficiary engagement is planned, communicated and executed so that the project results in a genuinely person-centered experience.

- j) Track/document how the information is used and by whom to make adjustments during implementation and evaluate the utility of the tool.
- k) Develop and/or alter existing video and text-based training materials for using the PHR. Materials must meet all criteria in section [II.B.2.b.](#) of this RFP.
- l) Provide telephone and web-based user support during regular business hours following deployment (described in section [II.B.2.A.iv.](#)) of the PHR system in the production environment until the end of the demonstration. This support includes assistance with authentication, training in use of the system, troubleshooting and ongoing technical support.
- m) See **Figure 1** below for an overview of the responsibilities of State Project Staff, MN.IT@DHS Staff, and the Collaborative.

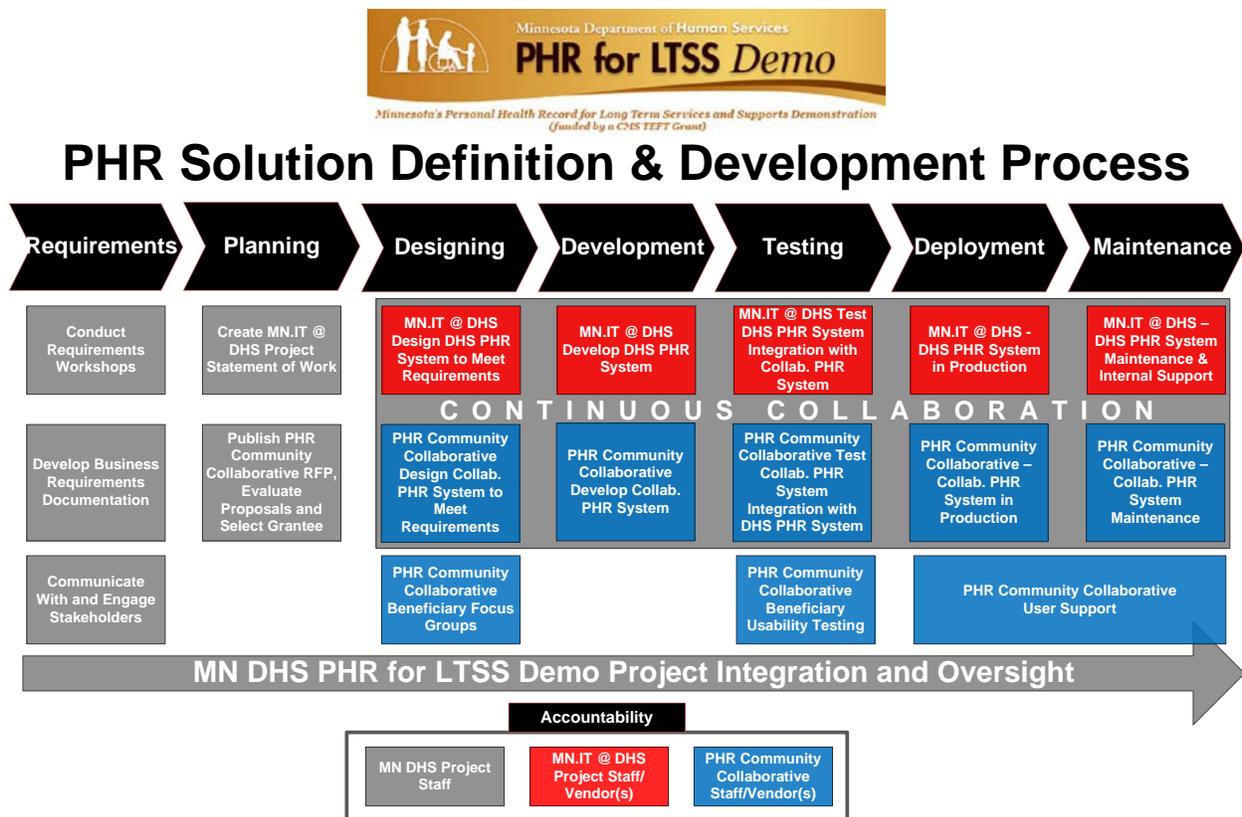


Figure 1

- n) Participate in testing an e-LTSS data standard within existing Collaborative systems and/or the PHR as required by DHS and the ONC S&I process, which may include the following:
 - i. Participate as required by the State in weekly ONC S&I calls.
 - ii. Identify Collaborative members who are using systems that could be used to test the e-LTSS standard.

- iii. Test the standard in the Collaborative member's systems if directed by the ONC S&I Framework.
- iv. Test the standard in the PHR modified by the Collaborative if required.

2. Deliverables:

- a) A secure, web-based Personal Health Record (PHR) system that will allow beneficiaries and legal representatives of MA funded LTSS who are served by Collaborative members to access information about their services, enter information about themselves online (e.g., notes, diary entries or other functions that may native to the PHR - this does not include making edits to DHS data), and securely share access to that information with others of their choosing. Detailed requirements for the PHR system are provided in the following requirements documents that are included as appendices to this document:
 - i. [Appendix A](#) - Business Requirements Document (BRD), which includes summaries of:
 - A. Business Function Model
 - B. Information Architecture
 - C. Application Integration Architecture
 - D. Functional Requirements
 - E. Information Requirements
 - F. User Experience Requirements
 - G. Integration Requirements
 - H. Security Requirements
 - I. Privacy Requirements
 - J. Performance Requirements
 - K. System Management Requirements
 - ii. [Appendix B](#) (available to download as a separate MS Excel document from the [PHR for LTSS Demo web page](#)) – Detailed Business Requirements Spreadsheets to be used for evaluation of proposals, including:
 - A. Functional Requirements - Beneficiary PHR Access and Use
 - Functional requirements define the actions that must be accommodated to meet the needs of the business
 - B. Functional Requirements - Case Manager PHR Access and Use
 - C. Functional Requirements - PHR Management, Operations, and Administration
 - D. User Experience Requirements - Beneficiary PHR Access and Use
 - E. User Experience Requirements - Case Manager PHR Access and Use
 - F. User Experience Requirements - PHR Management, Operations, and Administration
 - G. Non-Functional Performance Requirements
 - Non-functional requirements describe the parameters, structures, volumes or other needs that must be in place to achieve successful implementation of the requirements
 - H. Non-Functional System Management Requirements

- I. Non-Functional Security Requirements
 - J. Non-Functional Privacy Requirements
 - K. Non-Functional Interface Requirements
- iii. Review all attached requirements with your contracted PHR technology provider and indicate in your proposal how your PHR will or will not fulfill the stated requirements. The Collaborative’s contracted PHR technology provider must indicate in writing that it has thoroughly reviewed the requirements documentation, is willing to participate in the project, and that its technology solution is capable of meeting the RFP requirements (with exceptions noted in the Detailed Business Requirements Workbook). The form included as [Appendix I](#) must be signed by the vendor’s authorized representative and submitted as part of the Collaborative’s response to the RFP. Specific instructions for indicating how your proposed solution meets the requirements are provided in section [III.B.10.](#) of this RFP.
- iv. The PHR will be moved to production at a date agreed upon during contract negotiations and no later than April 3, 2017 and will provide the following general functionality:
- A. **Electronic view of DHS LTSS information** – users will be able to access and share some information that is already generated by DHS systems (and previously sent via US mail) within the PHR through a “DHS Profile Page”. Data from DHS systems that is displayed in the PHR will be “pushed” from those systems and will be read-only. Nothing that is entered by users of the PHR will be used to update DHS systems.
 - B. **Case manager and financial worker name and contact information** – users will be able to access and share case manager and financial worker name and contact information within the PHR.
 - C. **Text and/or email notifications (e.g. rules based messaging service)** – users will receive automated notifications via text to their cell phone and/or email generated by the PHR system when information from DHS is updated in their PHR.
 - D. **Discrete sharing of PHR information** – users will have control of access permissions, allowing them to share all or only selected portions of their PHR with users to whom they grant the right to access their PHR.
 - E. **Data entry** – users will be able to enter/update/delete information about themselves (e.g., notes, diary entries or other functions that may native to the PHR - this does not include making edits to DHS data) that can then be shared with other users at the discretion of the beneficiary or their legal representative.
 - F. **Electronic view of information** – users may be able to access and share read-only versions of Service Plans and Explanations of Benefits.
 - G. **Additional functionality (as feasible)** – users may be able to share additional information, including current lists of medications, allergies, problems, etc., as this information may be made available through EHRs of providers in the Community Collaborative. Respondents should indicate in their proposals

whether the additional information listed here could be securely shared through their PHR solution, as well as whether there are additional types of information not listed that could be shared in the PHR.

- b) Video and text-based training materials for using the PHR which meet the following minimum criteria:
- i. Provide clear, simple, understandable instructions that have undergone usability testing by actual beneficiaries/legal representatives to validate the usefulness of the materials for using the PHR, including:
 - A. User registration,
 - B. User authentication/sign-on,
 - C. Accessing information about the beneficiary's case manager,
 - D. Accessing other information from MN DHS systems in the PHR,
 - E. Sharing access to the PHR with others at the discretion of the beneficiary/legal representative,
 - F. Entering data about the beneficiary in appropriate fields,
 - G. Getting help/accessing user support options, and
 - H. Other functions available to the user.
 - ii. Meet or exceed accessibility guidelines in the State of Minnesota's [Accessibility Standard](#).
 - iii. Follow [Plain Language Guidelines](#) as described by the Plain Language Action and Information Network (PLAIN).
- c) Written processes and policies that ensure privacy and consent safeguards that comply with the [Health Insurance Portability and Accountability Act \(HIPAA\)](#), Minnesota Health Records Act, Title 38 Section 7332 Protections Confidentiality of Certain Medical Records and [MN Government Data Practices Act](#) regulations, and that fulfill the requirements of section 12.2 of the attached sample contract ([Appendix G](#)) are in place for the PHR.
- d) PHR Lessons Learned documentation produced at the end of the demonstration in a format to be determined by the State and contracted respondent, which includes project successes, failures and actions that could be taken to mitigate challenges encountered by the PHR Community Collaborative in future efforts of the State to provide PHRs or beneficiary portals to service recipients.
- e) Artifacts required by the ONC S&I Framework used for testing the e-LTSS Standard as indicated in [section II.B.1.n.](#) of this RFP. The Collaborative and State will work with the ONC S&I Framework to clearly define the characteristics of this deliverable as the project progresses.

III. Proposal Format

Proposals must conform to all instructions, conditions, and requirements included in the RFP. Responders are expected to examine all documentation and other requirements. Failure to observe the terms and conditions in completion of the proposal are at the responder's risk and may, at the discretion of the State, result in disqualification of the proposal for non-

responsiveness. Acceptable proposals must offer all tasks and deliverables identified in [section II.B.](#) of this RFP and agree to the contract conditions specified throughout the RFP.

A. Required Proposal Contents

Responses to this RFP must consist of all of the following components (see following sections for more detail on each component). Each of these components must be separate from the others and uniquely identified in the proposal.

1. Table of Contents

2. Proposal Requirements
 - a) Executive Summary
 - b) Description of the PHR Community Collaborative
 - c) Description of Each Collaborative Member
 - d) Description of Target Population
 - e) Project Goals, Activities and Implementation Plan
 - f) Solution Description
 - g) PHR Business Requirements Diagrams and Spreadsheets
 - h) Evaluation Plan
 - i) Budget Proposal
 - j) Professional Responsibility

Innovative Concepts (If Applicable)

3. Required Statements
 - a) Responder Information and Declarations
 - b) Exceptions to Terms and Conditions
 - c) Affidavit of Noncollusion
 - d) Trade Secret/Confidential Data Notification
 - e) Submission of Certified Financial Audit, IRS Form 990, or Most Recent Board-Reviewed Financial Statements
 - f) Disclosure of Funding Form
 - g) Human Rights Compliance:
 1. Affirmative Action Data Page
 2. Equal Pay Certificate
 - h) Certification and Restriction on Lobbying
 - i) Responder Commitment to Require Vendor Completion of DHS Security Questionnaire
 - j) PHR Vendor Review of Requirements Documentation Statement

Any additional information thought to be relevant, but not applicable to the prescribed format, may be included in the Appendix of your Proposal.

B. Proposal Requirements

The following will be considered minimum requirements of the proposal. Emphasis should be on completeness and clarity of content. All narrative components of the proposal must use a 12 point font.

1. Executive Summary:

Maximum length – 1 page

Complete this component of the proposal last, and demonstrate your understanding of the services requested in this RFP and any problems anticipated in accomplishing the work. Show your overall design of the project in response to achieving the tasks and deliverables as defined in this RFP. Specifically, demonstrate your familiarity with the project elements, its solutions to the problems presented, and knowledge of the requested services.

2. Description of the PHR Community Collaborative:

Maximum length – 3 pages plus attachments

You must include at a minimum a description of the scope of the PHR Community Collaborative, the governance structure and process for joint decision making. Identify the lead applicant organization for the grant. The applicant organization must meet the State's fiscal requirements and other grant participation requirements, including the ability to collect and submit data and manage staffing, facilities, communication, and other grant operations. The State must contract with the single entity making application. The degree to which that entity's decision-making ability and authority are clearly delineated will be a factor in evaluation.

Detail previous Collaborative efforts, if any, that include any Collaborative members. Include details of plans to pool and use funds in the project among the Collaborative members. Include steps that will lead to these outcomes in the work plan. Provide descriptions of specific, binding legal and financial commitments that are currently in place or will be initiated (and indicate which is the case for each) among the Collaborative members such as contracts, joint powers agreements, memoranda of understanding, data sharing agreements, Business Associate agreements, corporate by-laws, if any, etc. If you are selected as a grantee, you will be required to provide copies of these commitments to the State.

- Collaboratives which already have data sharing agreements in place between all partners can score up to 100% of possible points.
- Collaboratives which have data sharing agreements in place between some but not all partners can score up to 75% of possible points.
- Collaboratives which intend to execute data sharing agreements can score up to 50% of possible points.

Include information on the programs and activities of the Collaborative, the number of beneficiaries of MA served, geographic area served, percentage of MA beneficiaries served in the area, staff experience, and/or programmatic accomplishments. Describe the reasons why your Collaborative will be able to complete the services outlined in the RFP. Include a

brief history of your Collaborative and all strengths that you consider are an asset to your project. Provide evidence that your Collaborative has a current contract with the MN Department of Human Services (DHS) to serve as an Integrated Health Partnership (IHP) in Minnesota or has contracted with the MN Department of Health (MDH) to serve as an Accountable Care Organization (ACO). Demonstrate the length, depth, and applicability of all prior experience in HIT collaboration and providing the requested services. You may include letters of reference as attachments. Describe the qualifications of the leadership team. Demonstrate the skill and experience of lead staff and designate a project manager with experience in planning and providing the proposed services.

3. Description of Each Collaborative Member:

Maximum length – 1 page per Collaborative member (not including the Letter of Commitment)

Provide a description of each Collaborative member including:

- a) The programs and activities of the member organization, the number of beneficiaries of MA funded LTSS served, geographic area served, staff experience and/or programmatic accomplishments,
- b) A brief history of the organization and its strengths that are assets to the Collaborative, and
- c) The reasons why the organization is capable of effectively participating in the Collaborative.
- d) Attach a Letter of Commitment from the member organization which describes its role(s) and commitment to participate in the leadership team and the overall PHR Demonstration project.

4. Description of Target Population:

Maximum length – 1 page

Describe the needs of the target population, and indicate what group or groups of individuals will be targeted for services by the Collaborative. Indicate how those needs will be met by the Collaborative project. Include a description of the methods that will be used by the Collaborative to identify LTSS beneficiaries/legal representatives, caregivers, lead agency case managers, and providers who will participate in the activities defined in [section II.B.1.i.](#) of this RFP.

5. Project Goals, Activities and Implementation Plan:

Maximum length – 20 pages

Clearly define and discuss the goals and objectives of the project. Propose and describe specific milestones and outcomes that will be used to demonstrate the project's effectiveness. Address, in sufficient detail, how you will fulfill the expected Tasks and Deliverables required in [section II.B.](#) of this RFP. Simply repeating the outcomes and features and asserting that they will be performed is not an acceptable response. Detail how the project will be carried out in an effective and efficient manner including who will be involved, what resources are required, target dates for project activities and the

timeframe for completion. Propose and describe specific and measurable outcomes that will be used to show the demonstration's effectiveness.

6. Solution Description:

Maximum length – 10 pages

Describe your proposed PHR solution, both in summary and technical detail. Ensure that you include answers to the following questions:

- Does your Collaborative have an existing contract with a MN Certified HIESP? If so, name the HIESP and provide details about the relationship between the Collaborative and the HIESP.
- Are members of the Collaborative currently using certified CEHRT (Certified EHR Technology) or MN "Qualified" EHR systems? If so, name and describe the systems in use, as well as any existing interoperability with other Collaborative systems. Respondents should also be aware that CMS is considering "pre-certification" of Modular Medicaid IT Enterprise Solutions, according to a recently released [Request for Information \(RFI\)](#). If the EHR you are using is planning to pursue pre-certification, provide details about those plans in your proposal.
- Does the PHR already exist?
- Which of the three options described in [section II.B.1.d.i.](#) of this RFP will you use?
- In general terms, describe what current functionality in your PHR will meet the requirements of the grant, as well as what changes will be needed to the PHR to meet them.
- How will you approach modifications to the PHR?
- Who will be responsible for developing the required modifications and what are their qualifications to do so?
- How will case managers and providers access the information in the PHR? Provide confirmation that all beneficiaries/legal representatives, case managers and appropriate MA service providers will have access to the system without additional cost to them. Costs for their access must be included in the price of the PHR technology solution.
- Describe how the PHR Vendor(s) will be required to complete the "MN Department of Human Services Vendor Security Questionnaire" (see Appendix F) if required by the State, and to participate in good faith to resolve problems that may arise from the vendor security scoring process.
- Confirm that either the Collaborative's lead partner or the Collaborative's PHR vendor will agree to enter into a Data Sharing Agreement and Business Associate Agreement with DHS substantially similar to the one in [Appendix H](#). If the Collaborative's lead partner is a political subdivision subject to Minn. Stat. 466, then the Collaborative's PHR vendor must agree to enter into a Data Sharing Agreement and Business Associate Agreement substantially similar to the one in Appendix H.
- Include a written statement from the Collaborative's PHR vendor that it has thoroughly reviewed the requirements documentation, is willing to participate in

the project, and its technology solution is capable of meeting the RFP requirements (with exceptions noted in the Detailed Business Requirements spreadsheets).

7. PHR Business Requirements Diagrams and Spreadsheets:

Maximum length – 10 pages plus detailed requirements spreadsheets.

Working with your PHR technology vendor, describe in detail how your PHR solution will fulfill the requirements set forth in the Business Function Model, Information Architecture and Application Integration Architecture diagrams included in [Appendix A](#) of this RFP. Briefly describe the process you used to work with your PHR technology vendor to arrive at your responses.

Include copies of each of the following detailed business requirements spreadsheets included in [Appendix B](#) of this RFP (available to download as a separate MS Excel document from the [PHR for LTSS Demo web page](#)):

- a) Functional Requirements - Beneficiary PHR Access and Use
- b) Functional Requirements - Case Manager PHR Access and Use
- c) Functional Requirements - PHR Management, Operations, and Administration
- d) User Experience Requirements - Beneficiary PHR Access and Use
- e) User Experience Requirements - Case Manager PHR Access and Use
- f) User Experience Requirements - PHR Management, Operations, and Administration
- g) Non-Functional Performance Requirements
- h) Non-Functional System Management Requirements
- i) Non-Functional Security Requirements
- j) Non-Functional Privacy Requirements
- k) Non-Functional Interface Requirements

On each requirements spreadsheet, find the row(s) where “Collaborative” or “Both” is indicated in the “Accountability – Collaborative or MN.IT@DHS” column. These columns are NOT shaded. In those rows, fill in the “Collaborative Responses” section by entering the following information:

- “How Met”: Explain how the requirement will be met by the Collaborative PHR, or if the requirement cannot be met, indicate why. Indicate whether the required functionality already exists in the PHR, or if it would have to be added through the grant.
- “Level of Effort”: Indicate the level of effort that will be required for the Collaborative to deliver the requirement in its PHR.
- “Collaborative Solution Component Name”: Indicate the name of the specific element in the Collaborative PHR solution (application, module, plugin, etc.) where the requirement is addressed.
- “Notes”: Provide additional relevant information if needed.

The State has indicated in the “Priority” column for each requirement if it is “Critical,” “Important,” or “Useful.” See the description of the “Priority” field in the PHR Business Requirements Reference Guide at the beginning of the Detailed Requirements Workbook for definitions of these three values. Be sure that for every item that is marked “Critical,”

you indicate how you will meet that requirement, or suggest an alternative that will accomplish the intent set forth by the requirement.

8. Evaluation plan:

Maximum length – 2 pages.

The State is committed to funding services that produce a measurable result for the people of Minnesota. Develop indicators of the success and effectiveness of the project and be able to measure and evaluate them to determine outcomes. Include a plan to measure progress during the course of the project (process evaluation), including a feedback loop for correcting problems as they are encountered. Briefly describe the qualitative and quantitative methods used to gather information to measure the project's outcomes for beneficiaries/legal representatives and other users (including user feedback) as well as outcomes for the Collaborative (outcome evaluation). Describe the methods and criteria that will be used to measure whether the project goals and objectives have been achieved.

9. Budget proposal:

Please use the budget forms that are included in the “Detailed Business Requirements and Budget Forms” MS Excel file which can be downloaded from the [PHR for LTSS Demo web page](#). This section should specify the grant amount requested and detail all expenses for the proposed project. Describe and explain what the estimated costs pay for. Identify what other ancillary services are being provided that have costs associated with them and which components are essential to delivering minimum quality services. Include a budget narrative for the Collaborative and each subcontracting agency or vendor. Explain the proposed use of the grant funds and any non-grant funds that will be used for the project. The TEFT Notice of Grant Award (NGA) for the funds from CMS states, “The recipient is responsible for ensuring that no federal funds provided under this award are used to fund the same services or activities otherwise funded by the Federal government through any other funding mechanisms, such as any grants, cooperative agreements or other federal support for health information technology services.” Therefore all sources of funding that will be used to provide additional revenue for the Collaborative during the grant period must be identified on the “Non-Grant Funds” tab to demonstrate your compliance with the NGA.

Your explanation should provide sufficient detail to justify the total amount budgeted in each category. The project budget must be complete and reasonable, must link to the proposed project activities, and must specify how the amounts for each budget item were determined. Responders are encouraged to apply for only the amount needed for their proposed project. Over the course of the project, we will learn things from users and others that may result in the need to make changes to the PHR requirements. Therefore, understand that some portion of your budget may need to be adjusted to handle changes as they arise (i.e. handling change requests with a vendor). You may choose to set aside a reserve in your budget by category for adjustments. The budget must not exceed \$750,000 in grant funds. Budget proposals will be judged on efficient use of funds (that is, funds are being spent on direct services versus administrative costs, as detailed in their budget

proposal), level of appropriateness and commitment of collaborative partners, and overall cost-effectiveness.

a) Instructions for Preparing Budgets

i. Direct Costs

A “direct cost” is any cost that can be specifically identified with a particular project, program, or activity or that can be directly assigned to such activities relatively easily and with a high degree of accuracy. Direct costs include, but are not limited to, salaries, travel, equipment, and supplies directly benefitting the grant-supported project or activity.

ii. Personnel

Cost of individual staff salaries, wages and fringe benefits of applicant organization.

Budget justification: Specify the key staff by their first and last name, their titles, brief summary of project related duties, and their commitments to the project, based on full-time equivalent. Do not group staff together. Enter each individual separately. Provide a list of the elements that comprise fringe benefit costs, such as health insurance, FICA, retirement insurance. Explain the formula or rationale used to compute the cost of the fringe benefits listed in the budget proposed. Individuals who are not directly employed by the applicant organization but work on the grant should be listed under the “Contracts” line item. Consultant costs or professional fees should be included under the “Other” line item.

iii. Travel

Reimbursement to project staff for travel and subsistence expenses is to be made consistent with the current “Commissioner’s Plan” as promulgated by the Commissioner of Employee Relations. The Commissioner’s Plan states the current reimbursement rates for travel and subsistence expenses in Chapter 15: Expense Reimbursement. Travel rates must not exceed State of Minnesota rates.

- Lodging: Actual and reasonable costs.
- Mileage: Is based on Current Federal IRS mileage reimbursement rate. Mileage allowance may not exceed the State maximum, currently 54 cents per mile (2016). Include the total number of trips, destinations, purpose, length of stay, transportation cost (including mileage rates).
- Meals: In State: Breakfast- \$9.00, Lunch- \$11.00, Dinner- \$16.00
 - **Breakfast.** Breakfast reimbursements may be claimed if the employee leaves his/her temporary or permanent work location before 6:00 a.m. or is away from home overnight.
 - **Lunch.** Lunch reimbursements may be claimed if the employee is in travel status more than thirty-five (35) miles away from his/her

temporary or permanent work location or is away from home overnight.

- **Dinner.** Dinner reimbursements may be claimed only if the employee is away from his/her temporary or permanent work location until after 7:00 p.m. or is away from home overnight.

Do not include travel expenses for subcontractors or applicant/grantee's clients under travel, expenses incurred for clients list under other. Include the total number of trips, destinations, purpose, length of stay and transportation costs (including mileage rates).

All out-of-state travel and lodging requires prior State approval if State funds are used.

iv. Communication and Utilities

Cost of utilities, postage and communications.

Budget justification: Itemize and estimate anticipated charges for the project. Explain anticipated charges for Internet access, telephone (including cell phones) and fax services including the number of phone lines. Postage may include the cost of mass mailings or miscellaneous project mail. Detail the number of pieces, the postage per item cost and reason. For example - 100 letters x .49 = \$49 - letters to participating beneficiaries/legal representatives.

v. Building Space

Space rental

Budget justification: Specify whether the space occupied is rented or owned and whether or not the costs include utilities and other occupancy related charges. Include the number of square feet and the percentage of time used for grant purposes. For example; 1500 square feet x \$25/ft. x 50%=\$18,750.

vi. Equipment

The costs of all equipment to be acquired by the project. For all applicants "equipment" is non-expendable tangible personal property having a useful life of more than one year and acquisition cost of \$1,000 or more per unit. If the item does not meet the \$1,000 threshold, include it in your budget under supplies.

Budget justification: Equipment to be purchased with State funds must be justified as necessary for the conduct of the project. The equipment must be used for project related functions; the equipment, or a reasonable facsimile, must not be otherwise available to the applicant or its sub-grantees. An explanation including the cost of purchases, cost and terms of all rental agreements and purpose of equipment should be explained. The justification also must contain plans for the use or disposal of the equipment after the project ends.

vii. Supplies

Costs of all tangible expendable personal property (supplies) other than those included in equipment. Supplies include consumable commodities such as paper stock, pencils, print cartridges, photocopying, etc.

Budget justification: Provide general description of types of items included.

Explanation should indicate what items are included and how costs are estimated. Unallowable cost: "Printing," is utilizing a professional printing service to make a color or black and white digital printing for high quality brochures and professional looking manuals. Printing is not an allowable line item cost.

However, photocopying, a copy made on a copying machine and used in daily office operations is allowable.

viii. Contracts

Costs of all contracts, including procurement contracts (except those, which belong on other lines such as equipment, supplies etc.) and any contracts with organizations or individuals for the provision of technical assistance and other services.

Budget justification: For each line item listed under the heading of contracts, indicate the name of the organization, the purpose of the contract, and the dollar amount. If the name of the contractor, scope of work, and costs are not available or have not been negotiated, indicate when this information will be available. If necessary, attach an additional page for hard copy submissions or outline the detail within the "contracts" justification section.

ix. Other

Costs not included in the above line items. Such costs, where applicable, may include but are not limited to: insurance, medical and dental costs; non-contractual fees and travel paid directly to individual consultants; equipment rentals/lease; computer use; training and staff development costs (i.e. registration fees).

Budget justification: Provide an explanation for items in this category. Staff development/ conferences - Describe the types of activities for staff development costs for each (e.g. workshops, training, seminars, etc.) Specific costs for overnight travel and lodging should be explained if applicable. Client Transportation: Provide formula (including the number of units e.g., tokens, costs per unit, number of recipients, and months of service) for each specific area.

x. Administrative Overhead Costs

An "administrative overhead cost" is a cost for common or joint objectives that, therefore, cannot be readily identified with an individual, project, program or organizational activity. They generally include facilities operation and maintenance costs, depreciation and administrative expenses. Administrative overhead cost should not be requested in applications for capital and renovation

grants. When requesting administrative overhead costs, applicants/grantees should budget administrative overhead cost under the “other” category at a rate up to six percent of modified total of direct costs. Applicants/grantees need to provide detail in the “other” line item under the budget justification explaining costs associated with the request.

10. Professional Responsibility:

Maximum length – 1 page.

It is crucial that the State locate reliable grantees to serve our clients. The successful responder must be professionally responsible. Therefore, responders must include in their proposals satisfactory information regarding their professional responsibility.

Professional responsibility information includes providing information concerning any complaints filed with or by professional and/or state or federal licensing/regulatory organizations within the past six years against your organization or its employees relating to the provision of services. If such complaints exist, please include the date of the complaint(s), the nature of the complaint(s), and the resolution/status of the complaint(s), including any disciplinary actions taken.

All proposals must also include information about pending litigation and/or litigation resolved within the past two years that relates to the provision of services by your organization and/or its employees. If such litigation exists, please include the date of the lawsuit, nature of the lawsuit, and the dollar amount being requested as damages, and if resolved, what the resolution was (e.g. settled, dismissed, withdrawn by plaintiff, verdict for plaintiff with \$x damages awarded, verdict for responder, etc.).

Responder should also submit information which demonstrates recognition of their professional responsibility. This may include awards, certifications, and/or professional memberships.

The information collected from these inquiries will be used in the State’s determination of the award of the contract. It may be shared with other persons within the Minnesota Department of Human Services who may be involved in the decision-making process, and/or with other persons as authorized by law. You are not required to provide any of the above information. However, if you choose not to provide the requested information, your organization’s proposal may be found nonresponsive and given no further consideration. The State reserves the right to request any additional information to assure itself of a responder's professional status.

11. Adherence to the State’s Standard Contract Terms and Conditions

The Responder should adhere to the State’s standard contract terms and conditions as much as possible. Responders who make exceptions to the professional and technical contract template (see Appendix G), to sections related to **Indemnification** and **Information Privacy**

and Security (see Appendix H) in particular, will lose “technical points” during the proposal evaluation and selection process.

The Responder should complete the Exceptions to Terms and Conditions form,¹ and explicitly list all exceptions to State terms and conditions. On this form, the Responder must reference the professional and technical contract template section number, section heading, and page number for which an exception(s) is being taken. If no exceptions exist, state "NONE" specifically on this form. Whether or not exceptions are taken, the Responder must sign and date this form and submit it as part of their Proposal.

The evaluation team will rate this specific component using the formula below, which is consistent with the formula used in evaluating other technical proposal components:

Component Rating	Point Factor
<p>Excellent</p> <p>No exceptions exist. Exceptions to Terms and Conditions form states “NONE,” and is signed and dated.</p>	1.0
<p>Satisfactory</p> <p><u>One or more exceptions</u> are stated on Exceptions to Terms and Conditions form. Two or fewer of the exceptions are related to:</p> <p>1.Information Privacy and Security; 2. Indemnification.</p>	0.5
<p>Unacceptable</p> <p>Exceptions exist with <u>many exceptions specifically related to</u>:</p> <p>1.Information Privacy and Security; 2. Indemnification.</p>	0

C. Innovative Concepts (If Applicable)

The detailed needs and requirements for Responders in this RFP are not intended to limit the responder’s creativity in preparing a proposal. Responders may submit innovative ideas, new concepts, partnership arrangements, and optional features in response to this RFP. However, responder must still address the needs and requirements stated in this RFP. Submitting only a different idea instead of addressing the needs and requirements stated in the RFP will result in the responder’s proposal being found non-responsive and receiving no further consideration.

Any additional innovative concept submitted by a responder will only be reviewed after the required needs stated in the RFP have been addressed. The State will review such additional features to determine whether or not, in the State’s sole discretion, the features enhance the

¹ <https://edocs.dhs.state.mn.us/lfsrserver/Public/DHS-7019-ENG>

rest of the responder's proposal. If, at the State's sole discretion, it is determined that the additional innovative concepts would enhance the rest of the responder's proposal, the State may award bonus points to the responder's proposal in accordance with the evaluation process of this RFP.

D. Required Statements

Complete the correlating forms found in [eDocs](#) by clicking the links below and submit them as the "Required Statements" section of your proposal. You must use the current forms found in eDocs. Failure to use the most current forms found in eDocs in completion of the proposal are at the responder's risk and may, at the discretion of the State, result in disqualification of the proposal for non-responsiveness."

1. **Responder Information and Declarations ([Responder Information/Declarations Form DHS-7020-ENG²](#)):** Complete and submit the attached "Responder Information and Declarations" form. If you are required to submit additional information as a result of the declarations, include the additional information as part of this form. The Responder may fail the Required Statements Review in the event that the Responder does not affirmatively warrant to any of the warranties in the Responder Information and Declarations. Additionally, the State reserves the right to fail a Responder in the event the Responder does not make a necessary disclosure in the Responder Information and Declarations, or makes a disclosure which evidences a conflict of interest.
2. **Exceptions to RFP Terms ([Exceptions to Terms and Conditions Form- DHS-7019-ENG³](#)):** The contents of this RFP and the proposal(s) of the successful responder(s) may become part of the final contract if a contract is awarded. Each responder's proposal must include a statement of acceptance of all terms and conditions stated within this RFP or provide a detailed statement of exception for each item excepted by the responder.

Responders (or their contracted PHR technology vendors) who object to any condition of this RFP or the attached standard contract form (attached as [Appendix G](#)) or standard Data Sharing and Business Associate Agreement form (attached as [Appendix H](#)) must note the objection on the attached "Exceptions to RFP Terms" form. If a responder has no objections to any terms or conditions, the responder should write "None" on the form.

Much of the language reflected in the contract is required by statute or state policy. If you take exception to any of the terms, conditions or language in the contract, you must indicate those exceptions in your response to the RFP. Only those exceptions indicated in your response to the RFP will be available for discussion or negotiation. Please note, Section 13, "Intellectual Property" is subject to negotiation depending on the nature of the proposal submitted.

² <https://edocs.dhs.state.mn.us/lfs/Server/Public/DHS-7020-ENG>

³ <https://edocs.dhs.state.mn.us/lfs/Server/Public/DHS-7019-ENG>

Responders are cautioned that any exceptions to the terms of the standard State contract **which give the responder a material advantage over other responders may result in the responder's proposal being declared nonresponsive.** Proposals being declared nonresponsive will be considered failing and will receive no further consideration for award of the Contract. Also, proposals that take blanket exception to all or substantially all boilerplate contract provisions will be considered nonresponsive/failing proposals and rejected from further consideration for contract award.

3. **Affidavit of Noncollusion ([Affidavit of Noncollusion Form- DHS-7021⁴](#))** : Each responder must complete and submit the attached "Affidavit of Noncollusion" form. A proposal will fail this component if an Affidavit of Noncollusion is not submitted.
4. **Trade Secret/Confidential Data Notification ([Trade Secret/Confidential Data Notice Form- DHS-7015-ENG⁵](#))**: All materials submitted in response to this RFP will become property of the State and will become public record in accordance with Minnesota Statutes, section 13.591, after the evaluation process is completed. Pursuant to the statute, completion of the evaluation process occurs when the government entity has completed negotiating the contract with the successful responder. If a contract is awarded to the Responder, the State must have the right to use or disclose the trade secret data to the extent otherwise provided in the grant contract or by law.

If the responder submits information in response to this RFP that it believes to be trade secret/confidential materials, as defined by the Minnesota Government Data Practices Act, Minnesota Statutes, section 13.37, and the responder does not want such data used or disclosed for any purpose other than the evaluation of this proposal, the responder must:

- a) Clearly mark every page of trade secret materials in its proposal at the time the proposal is submitted with the words "TRADE SECRET" or "CONFIDENTIAL" in capitalized, underlined and bolded type that is at least 20 pt.; the State does not assume liability for the use or disclosure of unmarked or unclearly marked trade secret/confidential data;
- b) Fill out and submit the attached "Trade Secret/Confidential Information Notification Form," specifying the pages of the proposal which are to be restricted and justifying the trade secret designation for each item. If no material is being designated as protected, a statement of "None" should be listed on the form;
- c) Satisfy the burden to justify any claim of trade secret/confidential information. In order for a trade secret claim to be considered by the State, detailed justification that satisfies the statutory elements of Minnesota Statutes, section and the factors discussed in *Prairie Island Indian Community v. Minnesota Dept. of Public Safety*, 658 N.W.2d 876, 884-89 (Minn.App.2003) must be provided. Use of generic trade secret language encompassing substantial portions of the proposal or simple assertions of trade secret interest without substantive explanation of the basis therefore will be regarded as

⁴ <https://edocs.dhs.state.mn.us/lfs/Server/Public/DHS-7021-ENG>

⁵ <https://edocs.dhs.state.mn.us/lfs/Server/Public/DHS-7015-ENG>

- nonresponsive requests for trade secret exception and will not be considered by the State in the event of a data request is received for proposal information; and
- d) Defend any action seeking release of the materials it believes to be trade secret and/or confidential, and indemnify and hold harmless the State, its agents and employees, from any judgments awarded against the State in favor of the party requesting the materials, and any and all costs connected with that defense. This indemnification survives the State's award of a contract. In submitting a response to this RFP, the responder agrees that this indemnification survives as long as the trade secret materials are in the possession of the State. The State is required to keep all the basic documents related to its contracts, including selected responses to RFPs, for a minimum of six years after the end of the contract. Non-selected RFP proposals will be kept by the State for a minimum of one year after the award of a contract, and could potentially be kept for much longer.

The State reserves the right to reject a claim if it determines responder has not met the burden of establishing that the information constitutes a trade secret or is confidential. The State will not consider prices or costs submitted by the responder to be trade secret materials. Any decision by the State to disclose information designated by the responder as trade secret/confidential will be made consistent with the Minnesota Government Data Practices Act and other relevant laws and regulations. If certain information is found to constitute a trade secret/confidential, the remainder of the Proposal will become public; only the trade secret/confidential information will be removed and remain nonpublic.

The State also retains the right to use any or all system ideas presented in any proposal received in response to this RFP unless the responder presents a positive statement of objection in the proposal. Exceptions to such responder objections include: (1) public data, (2) ideas which were known to the State before submission of such proposal, or (3) ideas which properly became known to the State thereafter through other sources or through acceptance of the responder's proposal.

A proposal may fail if a Trade Secret/Confidential Data form is not completed and submitted with the proposal.

5. **Documentation to Establish Fiscal Responsibility:** The successful responder must be fiscally responsible. Therefore, responders must include in their proposals sufficient financial documentation to establish their financial stability.

IRS Form 990s.

If a responder is a not-for-profit organization that completed an IRS Form 990 in 2014, responder must submit its IRS Form 990.

If responder is concerned that its 2014 IRS Form 990 does not demonstrate its fiscal responsibility, it may supplement its application with any of the additional material described below. An IRS Form

990 is a federal tax return for nonprofit organizations. Nonprofit organizations that are recognized as exempt from federal income tax must file a Form 990 or Form 990 EZ if it has averaged more than \$25,000 in annual gross receipts over the past three tax years. Please also submit any information about any pending major accusations that could affect your financial stability.

Organizations without 2014 IRS Form 990s.

- (1) Organizations that have not completed an IRS Form 990 should submit a certified financial audit if they have one. A certified financial audit is a review of an organization's financial statements, fiscal policies and control procedures by an independent third party to determine if the statements fairly represent the organization's financial position and if organizational procedures are in accordance with Generally Accepted Accounting Principles (GAAP). Any organization with an annual revenue greater than \$750,000 is required to have a certified financial audit completed for any fiscal year in which they have total revenue of more than \$750,000.
- (2) If the organization does not have a certified financial audit, the organization must submit its most recent board-reviewed financial statements if it has a board.
- (3) If the organization does not have a certified financial audit or board-reviewed financial statements because it does not have a board, the organization should submit a certified statement of assets and debts (balance sheet) and evidence of cash flow including amounts in a checking account.

Responders may also include documentations of cash reserves to prevent shortages or delays in receipt of revenue, and/or any other documents sufficient to substantiate responsible fiscal management.

State may request additional information from these responders as necessary to determine financial stability.

All responders must submit any information about any pending major accusations that could affect your financial stability.

In the event a responder is either substantially or wholly owned by another corporate entity, the proposal must also include the most recent detailed financial report of the parent organization, and a written guarantee by the parent organization that it will unconditionally guarantee performance by the responder in each and every term, covenant, and condition of such contract as may be executed by the parties.

If the responder is a county government or a multi-county human services agency that has 1.) had an audit in the last year by the State Auditor or an outside auditing firm, or 2) meets the requirements of the Single Audit Act, the responder is not required to submit financial statements. However, the State reserves the right to request any financial information to assure itself of a county's financial status.

The information collected from these inquiries will be used in the State's determination of the award of the contract. It may be shared with other persons within the Minnesota Department of

Human Services who may be involved in the decision-making process, and/or with other persons as authorized by law. If you choose not to provide the requested information, your organization's proposal will be found nonresponsive and given no further consideration. The State reserves the right to request any additional information to assure itself of a responder's financial reliability. If a responder's submission in response to this component does not demonstrate its financial stability, the responder may fail this requirement and be disqualified from further consideration.

6. **Disclosure of Funding Form ([Disclosure of Funding Form- DHS-7018-ENG⁶](#))**

Per the Federal Funding Accountability and Transparency Act of 2006 "Transparency Act" or "FFATA" (Public Law 109-282), all entities and organizations receiving federal funds are required to report full disclosure of funding (United States Code, title 31, chapter 61, section 6101). The purpose of FFATA is to provide every American with the ability to hold the government accountable for each spending decision. The end result is to reduce wasteful spending in the government. The FFATA legislation requires information on federal awards to be made available to the public through a single, searchable website. Federal awards include grants, sub-grants, loans, awards, and delivery orders.

In order to comply with the federal statute, the Minnesota Department of Human Services is required to obtain and report by the grantee's Data Universal Numbering System (DUNS) number and determine if the grantee meets specific requirement which would require additional reporting items and to collect additional information on executive compensation if required. In order to comply with federal law and to collect this information, responders are required to fill out the Disclosure of Funding Form and submit it with their response. The form requires responders to provide their Data Universal Numbering System (DUNS) number. The Data Universal Numbering System (DUNS) number is the nine-digit number established and assigned by Dun and Bradstreet, Inc. (D&B) to uniquely identify business entities. If a responder does not already have a DUNS number, a number may be obtained from the D&B by telephone (currently 866-705-5711) or the Internet (currently at <http://fedgov.dnb.com/webform>). The responder must have a DUNS number before their response is submitted.

7. **Human Rights Compliance**

- A. **Affirmative Action. ([Affirmative Action Data Page- DHS-7016-ENG⁷](#)):** For all contracts estimated to be in excess of \$100,000, Responders are required to complete and submit the attached "Affirmative Action Data" page. As required by Minnesota Rules, part 5000.3600, "It is hereby agreed between the parties that Minnesota Statutes, section 363A.36 and Minnesota Rules, parts 5000.3400 - 5000.3600 are incorporated into any contract between these parties based upon this specification or any modification of it. A copy of Minnesota Statutes, section

⁶ <https://edocs.dhs.state.mn.us/lfs/Server/Public/DHS-7018-ENG>

⁷ <https://edocs.dhs.state.mn.us/lfs/Server/Public/DHS-7016-ENG>

363A.36 and Minnesota Rules, parts 5000.3400 - 5000.3600 are available upon request from the contracting agency.”

B. Equal Pay Certificate. ([Equal Pay Certificate- DHS-7075-ENG⁸](#))

1. Scope. Pursuant to Minnesota Statutes, section 363A.44, the State shall not execute a contract for goods or services or an agreement for goods or services in excess of \$500,000 with a business that has 40 or more full-time employees in the State of Minnesota or a state where the business has its primary place of business on a single day during the prior 12 months, unless the business has an equal pay certificate or it has certified in writing that it is exempt.

This section does not apply to a business, with respect to a specific contract, if the commissioner of administration determines that the requirements of this section would cause undue hardship on the business. This section does not apply to a contract to provide goods or services to individuals under Minnesota Statutes, chapters 43A, 62A, 62C, 62D, 62E, 256B, 256I, 256L, and 268A, with a business that has a license, certification, registration, provider agreement, or provider enrollment contract that is a prerequisite to providing those good or services.

2. Application. If your response to this RFP is or could be within the scope of Minnesota Statutes, section 363A.44, you must apply for an equal pay certificate by paying a \$150 filing fee and submitting an equal pay compliance statement to the Minnesota Department of Human Rights (“MDHR”). MDHR’s Equal Pay Certificate Application Form can be obtained at <http://mn.gov/mdhr/compliance/forms.html>. It is your sole responsibility to submit this statement to MDHR and – if required – apply for an equal pay certification before the due date of this proposal and obtain the certification prior to the execution of any resulting contract.

3. Revocation of Contract. If a contract is awarded to a business that does not have an equal pay certificate as required by Minnesota Statutes, section 363A.44, or is not in compliance with the laws identified within section 363A.44, MDHR may void the contract on behalf of the state, and the contract may be abridged or terminated by DHS upon notice that the MDHR has suspended or revoked the certificate of the business.

4. Equal Pay Certificate Compliance Form. You must complete the Equal Pay Certificate of Compliance Form and submit it with your proposal. The Equal Pay Certificate of Compliance Form can be obtained at <https://edocs.dhs.state.mn.us/lfserver/Public/DHS-7075-ENG>.

⁸ <https://edocs.dhs.state.mn.us/lfserver/Public/DHS-7075-ENG>

8. **Certification Regarding Lobbying ([Certificate Regarding Lobbying Form- DHS-7017-ENG](#)⁹):**
Federal money will be used or may potentially be used to pay for all or part of the work under the contract, therefore the responder must complete and submit the attached “Certification Regarding Lobbying” form.

9. **Responder Commitment to Require Vendor Completion of DHS Security Questionnaire:**
Print, complete and sign this document ([Appendix E](#)) and include it with your proposal. Participation in the Security Lifecycle Management Process is mandatory. Proposals that do not include this signed Commitment document will be disqualified as non-responsive. For your reference, a sample of the DHS Vendor Security Questionnaire is included as [Appendix E](#). You do NOT need to include a completed copy of the Questionnaire with your response – sign and include the Responder Commitment document only. The Questionnaire will be required at a later date if your proposal is selected for contracting.

10. PHR Vendor Review of Requirements Documentation Statement:

The Collaborative’s contracted PHR technology provider must indicate in writing that it has thoroughly reviewed the requirements documentation, is willing to participate in the project, and that its technology solution is capable of meeting the RFP requirements (with exceptions noted in the Detailed Business Requirements Workbook). The form included as [Appendix I](#) must be signed by the vendor’s authorized representative and submitted as part of the Collaborative’s response to the RFP. Specific instructions for indicating how your proposed solution meets the requirements are provided in section [III.B.10](#) of this RFP.

⁹ <https://edocs.dhs.state.mn.us/lfsrserver/Public/DHS-7017-ENG>

IV. RFP Process

A. Responders' Conference Webinar

A Responders' Conference Webinar will be held on Monday, August 8, 2016 at 2:00 p.m. Central Time via WebEx. Responders may also attend in person in Room #2390 of the Elmer L. Anderson Building in St. Paul, MN. Directions and parking information can be found [online](#). Contact information for the Webinar is as follows:

1. Click on [this link](#).
2. If requested, enter your name and email address.
3. Click "Join".
4. To join the teleconference only:
 - a) Provide your phone number when you join the meeting to receive a call back.
 - b) Alternatively, you can call:
Call-in toll-free number: 1-888-7425095 (US/Canada)
Call-in number: 1-619-3773319 (US/Canada)
Show global numbers, click [this link](#):
Conference Code: 520 767 8540

The Responder's Conference Webinar will serve as an opportunity for responders to ask specific questions of State staff concerning the project. Participation in the Responders' Conference Webinar is not mandatory but is recommended. Oral answers given at the conference will be non-binding. Written responses to questions asked at the webinar will be posted to the [PHR for LTSS Demo web page](#) after the conference.

B. Responders' Questions

Responders' questions regarding this RFP must be submitted in writing prior to 4:00 p.m. Central Time on Monday, August 15, 2016. All questions must be addressed to:

Request for Proposal Response

Attention: Tom Gossett, TEFT Grant Business Project Manager

Aging & Adult Services Division

Department of Human Services

PO Box 64976

St. Paul, MN 55164-0976

Phone (651) 451-6301

FAX #: (651) 431-7415

Questions may also be e-mailed to tom.l.gossett@state.mn.us.

Other personnel are NOT authorized to discuss this RFP with responders before the proposal submission deadline. **Contact regarding this RFP with any State personnel not listed above**

could result in disqualification. The State will not be held responsible for oral responses to responders.

Questions will be addressed in writing and made available to all identified prospective responders via the [PHR for LTSS Demo web page](#). Every attempt will be made to provide answers timely, with the intent that they are posted no later than August 19, 2016.

C. Proposal Submission

One (1) complete, digital copy of the proposal and all attachments must be submitted in .pdf format via email to the following email address: tom.l.gossett@state.mn.us. Proposals must be date and time-stamped by the DHS email system by 4:00 p.m. Central Time on Friday, September 2, 2016 to be considered. The State email system can receive attachments that are up to 20 MB in size. Please ensure that the file size of your submission is below 20 MB, or break it up and send it in multiple separate emails. If you need to send the submission in multiple emails, CLEARLY MARK the fact that you are sending the proposal in multiple emails. An email response will be provided to all timely submissions to confirm they have been received. Late proposals will not be considered and will be returned unopened to the submitting party. Faxed, mailed or hand-delivered proposals will not be accepted.

Clearly include the following in the subject line of the email used to submit the proposal: "PHR Community Collaborative Grant Proposal." All proposals must be submitted in a single .pdf document attached to an email. Any documents requiring signatures should be signed, scanned and included in the .pdf document.

All correspondence related to this RFP must be directed to:

Tom Gossett, TEFT Grant Business Project Manager
Aging & Adult Services Division
Department of Human Services
444 Lafayette Road N.
St. Paul, MN 55155
Phone (651) 431-2601
Email: tom.l.gossett@state.mn.us

It is solely the responsibility of each responder to assure that their proposal is delivered at the specific place, in the specific format, and prior to the deadline for submission. **Failure to abide by these instructions for submitting proposals may result in the disqualification of any non-complying proposal.**

V. Proposal Evaluation and Selection

A. Overview of Evaluation Methodology

1. All responsive proposals received by the deadline will be evaluated by the State. Proposals will be evaluated on “best value” as specified below, using a 1,000 point scale. The evaluation will be conducted in three phases:
 - a) Phase I Required Statements Review
 - b) Phase II Evaluation of Proposal Requirements
 - c) Phase III Selection of the Successful Responder(s)
2. During the evaluation process, all information concerning the proposals submitted, except identity, address, and the amount requested by responder, will remain non-public and will not be disclosed to anyone whose official duties do not require such knowledge.
3. Non-selection of any proposals will mean that either another proposal(s) was determined to be more advantageous to the State or that the State exercised the right to reject any or all Proposals. At its discretion, the State may perform an appropriate cost and pricing analysis of a responder's proposal, including an audit of the reasonableness of any proposal.

B. Evaluation Team

1. An evaluation team will be selected to evaluate responder proposals.
2. State and professional staff, other than the evaluation team, may also assist in the evaluation process. This assistance could include, but is not limited to, the initial mandatory requirements review, contacting of references, or answering technical questions from evaluators.
3. The State reserves the right to alter the composition of the evaluation team and their specific responsibilities.

C. Evaluation Phases

At any time during the evaluation phases, the State may, at the State’s discretion, contact a responder to (1) provide further or missing information or clarification of their proposal, (2) provide an oral presentation of their proposal, or (3) obtain the opportunity to interview the proposed key personnel. Reference checks may also be made at this time. However, there is no guarantee that the State will look for information or clarification outside of the submitted written proposal. Therefore, it is important that the responder ensure that all sections of the proposal have been completed to avoid the possibility of failing an evaluation phase or having their score reduced for lack of information.

1. Phase I: Required Statements Review

The Required Statements will be evaluated on a pass or fail basis. Responders must "pass" each of the requirements identified in these sections to move to Phase II.

2. Phase II: Evaluation of Technical Requirements of Proposals

- a) Points have been assigned to these component areas. The total possible points for these component areas are as follows:

Component Total	Possible Points
Executive Summary	50
Description of the PHR Community Collaborative	40
Description of Each Collaborative Member	40
Description of Target Population	80
Project Goals, Activities and Implementation Plan	120
Solution Description	120
PHR Business Requirements Diagrams and Spreadsheets	120
Evaluation plan	80
Budget proposal	300
Adherence to Standard Contract Terms	50
Total:	1000

- b) The evaluation team will review the components of each responsive proposal submitted. Each component will be evaluated on the responder's understanding and the quality and completeness of the responder's approach and solution to the problems or issues presented.
- c) After reviewing the proposals, the members of the evaluation team will rate each proposal component using the following scale:

Component Rating	Point Factor
Excellent	1.0
Very Good	0.8
Good	0.7
Satisfactory	0.5
Poor	0.3
Unacceptable	0.0

Upon determining which of the above ratings best describes the component being rated, the total possible points available for the component from paragraph (a) will be multiplied by the corresponding point factor.

Example: A “very good” rating (0.8) of a Proposed Budget worth a maximum of 300 points would receive a score of 240 (300 x 0.8=240)

- d) Innovative Concepts (Optional). Only after the Technical Requirements of the proposal have been ranked, and it has been determined that the responder’s proposal has passed

Phase II, will any innovative concepts submitted by the responder be reviewed. If a proposal is found not to have passed Phase II, any innovative concepts submitted will not receive consideration. The amount of bonus points to be given a proposal for innovative concepts is at the sole discretion of the State, depending on how much the State determines the ideas enhance the rest of the proposal. The amount given, if any, will be by consensus of the evaluation team. The State is under no obligation to give a proposal any bonus points in any situation. The maximum possible bonus points are 50, and will be applied to the Technical Requirements score up to the 1000 total points available.

3. Phase III: Selection of the Successful Responder(s)

- a) Only the proposals found to be responsive under Phases I and II will be considered in Phase III.
- b) The evaluation team will review the scoring in making its recommendations of the successful responder(s).
- c) The State may submit a list of detailed comments, questions, and concerns to one or more responders after the initial evaluation. The State may require said response to be written, oral, or both. The State will only use written responses for evaluation purposes. The total scores for those responders selected to submit additional information may be revised as a result of the new information.
- d) The evaluation team will make its recommendation based on the above-described evaluation process. The successful responder(s), if any, will be selected approximately one month after the proposal submission due date.

D. Contract Negotiations and Unsuccessful Responder Notice

If a responder(s) is selected, the State will notify the successful responder(s) in writing of their selection and the State's desire to enter into contract negotiations. Until the State successfully completes negotiations with the selected responder(s), all submitted proposals remain eligible for selection by the State.

In the event contract negotiations are unsuccessful with the selected responder(s), the evaluation team may recommend another responder(s).

After the State and chosen responder(s) have successfully negotiated a contract, the State will notify the unsuccessful responders in writing that their proposals have not been accepted. All public information within proposals will then be available for responders to review, upon request.

VI. Required Contract Terms and Conditions

A. Requirements. All responders must be willing to comply with all state and federal legal requirements regarding the performance of the grant contract. The requirements are set forth throughout this RFP and are contained in the attached grant contract in the Appendix.

B. Governing Law/Venue. This RFP and any subsequent contract must be governed by the laws of the State of Minnesota. Any and all legal proceedings arising from this RFP or any resulting contract in which the State is made a party must be brought in the State of Minnesota, District Court of Ramsey County. The venue of any federal action or proceeding arising here from in which the State is a party must be the United States District Court for the State of Minnesota.

C. Travel. Reimbursement for travel and subsistence expenses actually and necessarily incurred by the grantee as a result of the grant contract will be in no greater amount than provided in the current "Commissioner's Plan" promulgated by the commissioner of Minnesota Management and Budget. Reimbursements will not be made for travel and subsistence expenses incurred outside Minnesota unless it has received the State's prior written approval for out of state travel. Minnesota will be considered the home state for determining whether travel is out-of-state.

D. Preparation Costs. The State is not liable for any cost incurred by Responders in the preparation and production of a proposal. Any work performed prior to the issuance of a fully executed grant contract will be done only to the extent the responder voluntarily assumes risk of non-payment.

E. Contingency Fees Prohibited. Pursuant to Minnesota Statutes, section 10A.06, no person may act as or employ a lobbyist for compensation that is dependent upon the result or outcome of any legislation or administrative action.

F. Certification Regarding Debarment, Suspension, Ineligibility, and Voluntary Exclusion. Federal money will be used or may potentially be used to pay for all or part of the work under the contract, therefore the responder must certify the following, as required by the regulations implementing Executive Order 12549.

Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion -- Lower Tier Covered Transactions

Instructions for Certification

1. By signing and submitting this proposal, the prospective lower tier participant is providing the certification set out below.
2. The certification in this clause is a material representation of fact upon which reliance was placed when this transaction was entered into. If it is later determined that the prospective lower tier participant knowingly rendered an erroneous certification, in addition to other remedies available to the federal government, the department or agency with which this transaction originated may pursue available remedies, including suspension and/or debarment.

3. The prospective lower tier participant shall provide immediate written notice to the person to which this proposal is submitted if at any time the prospective lower tier participant learns that its certification was erroneous when submitted or had become erroneous by reason of changed circumstances.
4. The terms covered transaction, debarred, suspended, ineligible, lower tier covered transaction, participant, person, primary covered transaction, principal, proposal, and voluntarily excluded, as used in this clause, have the meaning set out in the Definitions and Coverages sections of rules implementing Executive Order 12549. You may contact the person to which this proposal is submitted for assistance in obtaining a copy of those regulations.
5. The prospective lower tier participant agrees by submitting this response that, should the proposed covered transaction be entered into, it shall not knowingly enter into any lower tier covered transaction with a person who is proposed for debarment under 48 C.F.R. part 9, subpart 9.4, debarred, suspended, declared ineligible, or voluntarily excluded from participation in this covered transaction, unless authorized by the department or agency with which this transaction originated.
6. The prospective lower tier participant further agrees by submitting this proposal that it will include this clause titled "Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion--Lower Tier Covered Transaction," without modification, in all lower tier covered transactions and in all solicitations for lower tier covered transactions.
7. A participant in a covered transaction may rely upon a certification of a prospective participant in a lower tier covered transaction that it is not proposed for debarment under 48 C.F.R. part 9, subpart 9.4, debarred, suspended, ineligible, or voluntarily excluded from covered transactions, unless it knows that the certification is erroneous. A participant may decide the method and frequency by which it determines the eligibility of its principals. Each participant may, but is not required to, check the List of Parties Excluded from Federal Procurement and Nonprocurement Programs
8. Nothing contained in the foregoing shall be construed to require establishment of a system of records in order to render in good faith the certification required by this clause. The knowledge and information of a participant is not required to exceed that which is normally possessed by a prudent person in the ordinary course of business dealings.
9. Except for transactions authorized under paragraph 5 of these instructions, if a participant in a covered transaction knowingly enters into a lower tier covered transaction with a person who is proposed for debarment under 48 C.F.R. 9, subpart 9.4, suspended, debarred, ineligible, or voluntarily excluded from participation in this transaction, in addition to other remedies available to the federal government, the department or agency with which this transaction originated may pursue available remedies, including suspension and/or debarment.

Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion - Lower Tier Covered Transactions

1. The prospective lower tier participant certifies, by submission of this proposal, that neither it nor its principals is presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by any Federal department or agency.
2. Where the prospective lower tier participant is unable to certify to any of the statements in this certification, such prospective participant shall attach an explanation to this proposal.

G. Insurance Requirements

1. Responder shall not commence work under the grant contract until they have obtained all the insurance described below and the State of Minnesota has approved such insurance. All policies and certificates shall provide that the policies shall remain in force and effect throughout the term of the grant contract.

2. Responder is required to maintain and furnish satisfactory evidence of the following insurance policies:

a. **Workers' Compensation Insurance:** Except as provided below, responder must provide Workers' Compensation insurance for all its employees and, in case any work is subcontracted, responder will require the subcontractor to provide Workers' Compensation insurance in accordance with the statutory requirements of the State of Minnesota, including Coverage B, Employer's Liability. Insurance minimum amounts are as follows:

\$100,000 – Bodily Injury by Disease per employee

\$500,000 – Bodily Injury by Disease aggregate

\$100,000 – Bodily Injury by Accident

If Minnesota Statute, section 176.041 exempts responder from Workers' Compensation insurance or if the responder has no employees in the State of Minnesota, responder must provide a written statement, signed by an authorized representative, indicating the qualifying exemption that excludes responder from the Minnesota Workers' Compensation requirements.

If during the course of the grant contract the responder becomes eligible for Workers' Compensation, the responder must comply with the Workers' Compensation Insurance requirements herein and provide the State of Minnesota with a certificate of insurance

b. **Commercial General Liability:** Responder is required to maintain insurance protecting it from claims for damages for bodily injury, including sickness or disease, death, and for care and loss of services as well as from claims for property damage, including loss of use which may arise from operations under the grant contract whether the operations are by the responder or by a

subcontractor or by anyone directly or indirectly employed by the responder under the grant contract. Insurance minimum amounts are as follows:

\$2,000,000 – per occurrence

\$2,000,000 – annual aggregate

\$2,000,000 – annual aggregate – Products/Completed Operations

The following coverages shall be included:

Premises and Operations Bodily Injury and Property Damage

Personal and Advertising Injury

Blanket Contractual Liability

Products and Completed Operations Liability

Other; if applicable. Please list _____.

State of Minnesota named as an Additional Insured, to the extent permitted by law.

c. Commercial Automobile Liability: Responder is required to maintain insurance protecting the responder from claims for damages for bodily injury as well as from claims for property damage resulting from ownership, operation, maintenance or use of all owned, hired, and non-owned autos which may arise from operations under this grant contract, and in case any work is subcontracted the responder will require the subcontractor to provide Commercial Automobile Liability. Insurance minimum amounts are as follows:

\$2,000,000 – per occurrence Combined Single limit for Bodily Injury and Property Damage

In addition, the following coverages should be included:

Owned, Hired, and Non-owned Automobile

d. Professional/Technical, Errors and Omissions, and/or Miscellaneous Liability Insurance

This policy will provide coverage for all claims the responder may become legally obligated to pay resulting from any actual or alleged negligent act, error, or omission related to responder's professional services required under the grant contract.

Responder is required to carry the following minimum amounts:

\$2,000,000 – per claim or event

\$2,000,000 – annual aggregate

Any deductible will be the sole responsibility of the responder and may not exceed \$50,000 without the written approval of the State. If the responder desires authority from the State to have a deductible in a higher amount, the responder shall so request in writing, specifying the amount of the desired deductible and providing financial documentation by submitting the

most current audited financial statements so that the State can ascertain the ability of the responder to cover the deductible from its own resources.

The retroactive or prior acts date of such coverage shall not be after the effective date of this grant contract and responder shall maintain such insurance for a period of at least three (3) years, following completion of the work. If responder discontinues such insurance, then extended reporting period coverage must be purchased to fulfill this requirement.

e. Blanket Employee Theft/Employee Dishonesty Insurance.

Responder is required to obtain a blanket employee theft/employee dishonesty policy in at least the total amount of the first year's grant award as either an addendum on its property insurance policy, or if it is not feasible to include it as an addendum to a property insurance policy, as a stand-alone employee theft/employee dishonesty policy. The State will be named as both a joint payee and a certificate holder on the property insurance policy addendum or on the stand-alone employee theft/employee dishonesty policy, whichever is applicable. Only in cases in which the first year's grant award exceeds the available employee theft/employee dishonesty coverage may responders provide blanket employee theft/employee dishonesty insurance in an amount equal to either 25% of the yearly grant amount, or the first quarterly advance amount, whichever is greater. Upon execution of a grant contract, the responder must furnish the State with a certificate of employee theft/employee dishonesty insurance. This requirement does not apply to grant contracts with the University of Minnesota, counties, school districts or reservations.

3. Additional Insurance Conditions:

- Responder's policy(ies) shall be primary insurance to any other valid and collectible insurance available to the State of Minnesota with respect to any claim arising out of responder's performance under this grant contract;
- If responder receives a cancellation notice from an insurance carrier affording coverage herein, responder agrees to notify the State of Minnesota within five (5) business days with a copy of the cancellation notice, unless responder's policy(ies) contain a provision that coverage afforded under the policy(ies) will not be cancelled without at least thirty (30) days advance written notice to the State of Minnesota;
- Responder is responsible for payment of grant contract related insurance premiums and deductibles;
- If Responder is self-insured, a Certificate of Self-Insurance must be attached;
- Include legal defense fees in addition to its liability policy limits, with the exception of V.G.2.d. above; and

- Obtain insurance policies from an insurance company having an “AM BEST” rating of A- (minus); Financial Size Category (FSC) VII or better and must be authorized to do business in the State of Minnesota; and
- An Umbrella or Excess Liability insurance policy may be used to supplement the responder’s policy limits to satisfy the full policy limits required by the grant contract.

4. The State reserves the right to immediately terminate the grant contract if the responder is not in compliance with the insurance requirements and retains all rights to pursue any legal remedies against the responder. All insurance policies must be open to inspection by the State, and copies of policies must be submitted to the State’s authorized representative upon written request.

5. The successful responder is required to submit Certificates of Insurance acceptable to the State of Minnesota as evidence of insurance coverage requirements prior to commencing work under the grant contract.

I. Accessibility Standards

Any information systems, tools, information content, and/or work products, including the response to this solicitation/contract, applications, web sites, video, learning modules, webinars, presentations, etc., whether commercial, off-the-shelf (COTS) or custom, purchased or developed, must comply with the Minnesota IT Accessibility Standards effective September 1, 2010, as updated on October 3, 2013. This standard requires in part, compliance with the Web Content Accessibility Guidelines (WCAG) 2.0 (Level AA) and Section 508 Subparts A-D.

Information technology deliverables and services offered must comply with the [MN.IT Services Accessibility Standards](#) . The relevant requirements are contained under the “Standards” tab. Information technology deliverables or services that do not meet the required number of standards or the specific standards required may be rejected and may not receive further consideration.

VII. State’s Authority

Notwithstanding anything to the contrary, the State may:

- A. Reject any and all proposals received in response to this RFP;
- B. Disqualify any responder whose conduct or proposal fails to conform to the requirements of this RFP;
- C. Have unlimited rights to duplicate all materials submitted for purposes of RFP evaluation, and duplicate all public information in response to data requests regarding the proposal;

D. Select for contract or for negotiations a proposal other than that with the lowest cost or the highest evaluation score;

E. Consider a late modification of a proposal if the proposal itself was submitted on time and if the modifications were requested by the State and the modifications make the terms of the proposal more favorable to the State, and accept such proposal as modified;

F. At its sole discretion, reserve the right to waive any non-material deviations from the requirements and procedures of this RFP;

G. Negotiate as to any aspect of the proposal with any responder and negotiate with more than one responder at the same time, including asking for responders' "Best and Final" offers;

H. Extend the grant contract, in increments determined by the State, not to exceed a total contract term of five years; and

I. Cancel the RFP at any time and for any reason with no cost or penalty to the State.

J. Correct or amend the RFP at any time with no cost or penalty to the State. The State will not be liable for any errors in the RFP or other responses related to the RFP.

Remainder of the page intentionally left blank (Appendices follow).

Appendix A: Business Requirements Document



Minnesota Department of Human Services

PHR for LTSS *Demo*

*Minnesota's Personal Health Record for Long Term Services and Supports Demonstration
(funded by a CMS TEFT Grant)*

Business Requirements Document

Revision History

Date	Version	Description of Changes	Author
Feb 2-20 2015	1-4	Initial internal draft outlines	KPMG Team
23 Feb 2015	5	Incomplete draft provided to DHS	KPMG Team
24 Feb 2015	6-7	Internal drafts for KPMG review	KPMG Team
25 Feb 2015	8	First Formal Draft for Review and Update by DHS Core Team	KPMG Team
3 Apr 2015	9	Updates from DHS Core Team	PM
7 Apr 2015	10	Updated Glossary, added MAXIS as a source system	BA
10 Apr 2015	11	Final updates for RFP publication	PM
21 Jun 2016	12	Edits before publication of 2 nd round RFP	PM

TABLE OF CONTENTS

1. PROJECT DEMOGRAPHICS	5
2. PROJECT SUMMARY	6
2.1 BACKGROUND.....	6
2.2 BUSINESS LEVEL GOALS/COST BENEFITS.....	6
2.3 PROJECT CRITICAL SUCCESS FACTORS.....	7
2.4 PROJECT MEASURES	7
2.5 ACCEPTANCE CRITERIA.....	8
2.6 STAKEHOLDERS.....	8
2.7 PROJECT SCOPE.....	11
2.7.1 <i>Scope Accountability</i>	11
2.7.2 <i>In Scope</i>	14
2.7.3 <i>Out of Scope</i>	17
2.8 ASSUMPTIONS, DEPENDENCIES, AND CONSTRAINTS	17
2.8.1 <i>Assumptions</i>	17
2.8.2 <i>Dependencies</i>	18
2.8.3 <i>Constraints</i>	18
3. PROJECT OVERVIEW	18
3.1 CURRENT PROCESS.....	19
3.2 PROPOSED PROCESS.....	19
4. BUSINESS REQUIREMENTS	22
4.1 FUNCTIONAL REQUIREMENTS.....	22
4.1.1 <i>PHR User Roles</i>	22
4.1.2 <i>Beneficiary PHR Access and Use – Functional Requirements</i>	22
4.1.3 <i>Case Manager and LTSS Provider PHR Access and Use – Functional Requirements</i>	23
4.1.4 <i>PHR Management, Operations, and Administration – Functional Requirements</i>	24
4.2 USER EXPERIENCE REQUIREMENTS	24
4.2.1 <i>PHR User Experience Requirements for Beneficiaries and Legal Representatives</i>	25
4.2.2 <i>PHR User Experience Requirements for Case Managers and LTSS Providers</i> .	25
4.2.3 <i>PHR User Experience Requirements for System Administrators</i>	25
4.3 TARGET ARCHITECTURE	26
4.3.1 <i>Architecture Context</i>	26
4.3.2 <i>Target Solution Architecture</i>	26
4.3.3 <i>PHR Infrastructure</i>	28
4.3.4 <i>Source Systems</i>	29
4.4 INFORMATION REQUIREMENTS	29
4.5 INTEGRATION REQUIREMENTS.....	32
4.6 SECURITY REQUIREMENTS	36
4.7 PRIVACY REQUIREMENTS	37
4.8 PERFORMANCE REQUIREMENTS.....	37
4.9 SYSTEMS MANAGEMENT REQUIREMENTS.....	37

5. SYSTEM AND USER ACCEPTANCE TESTING	39
5.1 TESTING PHASES.....	39
5.1.1 <i>Unit Testing</i>	39
5.1.2 <i>Integration Testing</i>	39
5.1.3 <i>System Testing</i>	39
5.1.4 <i>Regression Testing</i>	39
5.1.5 <i>User Acceptance Testing</i>	39
5.1.6 <i>Usability Testing</i>	40
5.2 TEST SIGN-OFF RESPONSIBILITY	40
5.3 MAJOR BUSINESS PROCESSES/SCENARIOS	40
5.3.1 <i>Beneficiary PHR Access and Use</i>	40
5.3.2 <i>Case Manager and LTSS Provider PHR Access and Use</i>	40
5.3.3 <i>PHR Management, Operations, and Administration</i>	40
5.4 EXPECTATIONS OF DATA PROVIDED FOR TESTING	40
5.4.1 <i>Test Data</i>	40
5.4.2 <i>Time for Testing</i>	41
5.4.3 <i>Pass/Fail Scores and Criteria</i>	41
6. OPERATIONAL IMPLEMENTATION CONSIDERATIONS	42
6.1 OPERATIONAL IMPACTS	42
6.2 DOCUMENTATION PLAN	42
6.3 TRAINING IMPACT.....	44
7. DEPLOYMENT CONSIDERATIONS	45
8. PROJECT CHANGE MANAGEMENT	45
9. REFERENCES	46
10. PHR FOR LTSS DEMO – GLOSSARY AND SELECTED ACRONYMS	47
APPENDIX – DETAILED BUSINESS REQUIREMENTS WORKBOOK.....	53

1. PROJECT DEMOGRAPHICS

Project ID#	PHR for LTSS Demo
Project Name and Description	Personal Health Record (PHR) for Long Term Services and Supports (LTSS) Demonstration.
Business Segment and Department Name	Minnesota Department of Human Services (DHS)
Business Sponsor(s)	Kari Benson (Director, Aging & Adult Services Division) and Alex Bartolic (Director, Disability Services Division)
Business Owner(s)	Rolf Hage (Supervisor, Resource Development Team, DHS)
Key Business Partners	Centers for Medicare & Medicaid Services (CMS) MN.IT @ DHS MN Office of Health Information Technology (OHIT) Aging and Disability service waivers (DHS) Service Management Agencies (Counties, Tribes) Managed Care Organizations Service Providers Advocates and Beneficiaries.
Key Business Contacts	Tom Gossett (TEFT Grant Business Project Manager, DHS) Rick Bagley (Systems Architect, MN.IT @ DHS) Greg Linden (CIO, Stratis Health) Catalina Adamez-Smith (IT Project Manager, MN.IT @ DHS) Kari Guida (Sr. Health Informatician, MN Department of Health) Val Cooke (Manager, Nursing Facility Rates & Policy, DHS) Dan Newman (Health Care Prog. Mgr., DHS)
Document Author(s)	KPMG Team: Tom Drzich, Sumit Chaterjee, Gerardo Amaya, Sandy McBride
Business Analyst(s)	Scott Winkels (Business Analyst, MN.IT @ DHS)

2. PROJECT SUMMARY

2.1 Background

A June 2013 DHS Continuing Care Administration Report, [Expansion of Electronic Health Records for Long Term Services and Supports](#), found that expanding the use of [Electronic Health Records \(EHR\)](#) for [Long Term Services and Supports \(LTSS\)](#) beneficiaries would result in improved care transitions and care coordination, improved data analytics within DHS systems, and would help ensure a person-centered, beneficiary-owned approach to data. The State is pursuing ways to use [Health Information Technology \(HIT\)](#) to further this goal. DHS applied for funding from CMS to demonstrate use of HIT through a [Personal Health Record \(PHR\)](#) in October 2013.

DHS is one of nine state Medicaid agencies awarded a four year CMS Testing Experience and Functional Tools (TEFT) Grant in 2014. The State has opted to participate in all four aspects of the CMS TEFT Grant program, which requires that it accomplish the following goals:

- Demonstrate use of Personal Health Record (PHR) systems with beneficiaries of [Community-Based Long Term Services and Supports \(CB-LTSS\)](#); and
- Identify, evaluate and harmonize an electronic Long Term Services and Supports (e-LTSS) standard in conjunction with the [Office of the National Coordinator's \(ONC\) Standards and Interoperability \(S&I\) Framework](#); and
- Field test a beneficiary experience survey within multiple CB-LTSS programs for validity and reliability; and
- Field test a modified set of Functional Assessment Standardized Items (FA SI) functional assessment measures for use with beneficiaries of CB-LTSS programs.

This Business Requirements Document will be used by a MN PHR Community Collaborative (Collaborative) to work closely with the State and Minnesota's Information Technology Agency (MN.IT @ DHS) staff to accomplish the first two goals of the CMS TEFT Grant.

2.2 Business Level Goals/Cost Benefits

In addition to the high level program goals of the demo, there are several other key objectives for the PHR for LTSS Demo. These objectives include a variety of technical and operational objectives. The PHR for LTSS Demo will:

- Determine what information about LTSS beneficiaries is currently in DHS systems and how that information can be made available to them, subject to privacy and consent rules.
- Make information in DHS systems available to LTSS beneficiaries in a way that is person-centered, ensuring that it is understandable, useful, accessible and shareable.
- Provide LTSS beneficiaries with a Personal Health Record, which can contain information from DHS, primary, acute and post-acute care providers, as well as from the beneficiaries themselves.
- Leverage data integration efforts for State quality/population health data and analytics.

- Contain information on a beneficiary's LTSS records that is exchangeable (e.g., results of assessment data for home care, transportation, nursing facility, hospice, [Elderly Waiver](#), [Developmental Disabilities Waiver](#), [Community Alternative Care Waiver](#), [Community Alternatives for Disabled Individuals Waiver](#) and [Brain Injury Waiver](#) services).
- Provide integrated client case data from DHS programs (based on or aligned with the DHS Enterprise Systems Modernization vision to the extent possible), including data from systems containing CB-LTSS beneficiary information (e.g., MMIS, MnCHOICES, SSIS, MAXIS, possibly others).
- Allow a beneficiary/legal representative to enter information into their system (e.g., notes, diary entries or other functions that may be native to the PHR - this does not include making edits to DHS data).
- Align with Consolidated Content Document Architecture (C-CDA) HL7 standards where applicable.
- Align with e-LTSS standards where applicable.
- Leverage other existing data standards where applicable.
- Embed and align with privacy requirements.
- Provide access to and sharing of information that is as current as possible.
- Leverage/complement existing EHR and tethered PHR portals that have already been implemented in Minnesota.
- Consider consolidated models (data replicated from identified sources into a shared PHR database) and federated models (data accessed from multiple identified sources).

2.3 Project Critical Success Factors

- Relevant data from DHS source systems are accurately and consistently aggregated and characterized for publication to the Collaborative PHR.
- Aggregated and characterized data from DHS systems are securely transported to the Collaborative PHR at regular, agreed upon intervals.
- DHS data are securely stored in the Collaborative PHR's data store (e.g., [Clinical Data Repository](#)).
- The Collaborative PHR securely provides and maintains access permissions for all users.
- The Collaborative PHR displays data from DHS systems for users in a way that is accessible, understandable and useful to beneficiaries/legal representatives.
- Beneficiaries/legal representatives use the Collaborative PHR to access DHS data.

2.4 Project Measures

Project measurement will be conducted throughout the course of the project and will include factors such as those listed in the table below.

Metric	Target
Cost	\$1,188,060 - Project goals are accomplished within the following cost constraints: <ul style="list-style-type: none"> • MN.IT @ DHS Project - \$438,060 • PHR Community Collaboratives - \$750,000 (total)
Schedule	PHR is in production by 4/1/2017 (or earlier)
Output	DHS data are accurately and consistently characterized within the Data Aggregator with minimal errors
Errors	After original launch, less than 5% of time is spent fixing problems
Beneficiary/Legal Representative Use of PHR	At least 25% of targeted beneficiaries/legal guardians access the PHR at least twice between product launch and 3/31/2018
Beneficiary/Legal Representative Satisfaction	At least 70% of beneficiaries/legal guardians who access the PHR indicate they are satisfied with its functionality
Case Manager Satisfaction	At least 80% of Case Managers who use the PHR indicate they are satisfied with its functionality

2.5 Acceptance Criteria

The PHR Demonstration Solution will be accepted based on how well it is considered to conform to the scope specified in section 2.7, how well it conforms to the constraints defined in section 2.8.3, and how well it meets the requirements specified in section 4 and the appended Detailed Business Requirements Workbook.

2.6 Stakeholders

The following is a comprehensive inventory of stakeholders that may be involved in the design, use or evaluation of the PHR. This inventory is broad in nature as it identifies all of the candidate stakeholder groups; however the demonstration is likely to include only a subset of these groups.

Stakeholder	Role	Value to the Stakeholder
Beneficiaries	Medical Assistance Beneficiaries	<ol style="list-style-type: none"> 1. Single source for health care and LTSS history 2. Reduce potential errors during patient intake 3. Tool to enable better health management-chronic disease management 4. Improved beneficiary engagement 5. Improved care coordination 6. Available in emergency situations 7. Streamlined intake and care transition process 8. Streamlined Family Health Management 9. Better understanding of health care and social services received.

Stakeholder	Role	Value to the Stakeholder
		10. Secure mechanism for sharing information with appropriate parties
Hospital/Health System	Healthcare Service Provider	<ol style="list-style-type: none"> 1. May provide access to medical history for better diagnosis 2. Improved patient engagement 3. Improved health management (shared lab results, medication lists, etc.) 4. Improved care coordination 5. Available in emergency situations 6. Captures data outside of the medical office (e.g., exercise, over the counter drugs etc.). 7. Streamlined intake process 8. Reduced administrative tasks/costs 9. Meaningful Use Requirement 10. Improved managed care results 11. Enables beneficiaries to securely share relevant information from their PHR with the hospital, and share relevant hospital information with other providers, guardians/caregivers and other designees
Clinic	Healthcare Service Provider	<ol style="list-style-type: none"> 1. May provide access to medical history for better diagnosis 2. Improved patient engagement 3. Improved health management (shared lab results, medication lists, etc.) 4. Improved care coordination 5. Available in emergency situations 6. Captures data outside of the medical office (e.g., exercise, over the counter drugs etc.). 7. Streamlined intake process 8. Reduced administrative tasks/costs 9. Enables beneficiaries to securely share relevant information from their PHR with the clinic, and share relevant clinic information with other providers, guardians/caregivers and other designees
Long Term Services and Supports – Residential Providers	LTSS Provider (Skilled Nursing Facilities, Assisted Living, Intermediate Care Facilities)	<ol style="list-style-type: none"> 1. May provide access to medical history for better diagnosis 2. Improved health management (shared lab results) 3. Improved care coordination 4. Available in emergency situations 5. Captures data outside of the medical office (e.g., exercise, over the counter drugs etc.). 6. Streamlined intake process 7. Reduced administrative tasks/costs 8. Improved managed care results. 9. Enables beneficiaries to securely share relevant information from their PHR with the LTSS residential provider, and share relevant LTSS residential provider information with other providers, guardians/caregivers and other designees
Long Term Services and Supports – Home & Community Based Providers	LTSS Provider (Home Care, Hospice, Chore, Waiver Services)	<ol style="list-style-type: none"> 1. May provide access to medical history for better diagnosis 2. Improved health management (shared lab results) 3. Improved care coordination 4. Available in emergency situations 5. Captures data outside of the medical office (e.g., exercise, over the counter drugs etc.).

Stakeholder	Role	Value to the Stakeholder
		<ul style="list-style-type: none"> 6. Streamlined intake process 7. Reduced administrative tasks/costs 8. Improved managed care results 9. Enables beneficiaries to securely share relevant information from their PHR with the LTSS HCBS provider, and share relevant LTSS HCBS provider information with other providers, guardians/caregivers and other designees
Private Payer of non-public portion of MA Services	Payer	<ul style="list-style-type: none"> 1. May provide access to medical history for better diagnosis 2. Improved health management (shared lab results, etc.) 3. Improved care coordination 4. Available in emergency situations 5. Captures data outside of the medical office (e.g., exercise, over the counter drugs etc.). 6. Lower costs of care 7. Ensures beneficiaries can see information about services received from all providers, ensuring that private pay responsibility is accurately calculated
HIE Service Provider	HIE Operator	<ul style="list-style-type: none"> 1. Increased HIE usage 2. Potential reference if the HIE is not available 3. Helps to move various parties forward toward meaningful exchange of health and service information, including e-LTSS data
Lead Agencies (Counties/Tribes)	MDH, DHS service delivery agents	<ul style="list-style-type: none"> 1. Healthier population 2. Lower costs 4. Enables beneficiaries to securely share relevant information from their PHR with the County/Tribe/Lead Agency, and share relevant service information with other providers, guardians/caregivers and other designees
MN Dept. of Health	Program Manager, Payer	<ul style="list-style-type: none"> 1. Healthier population 2. Lower costs of care 3. Helps to move various parties forward toward meaningful exchange of HIE, including e-LTSS data
MN Dept. of Human Services	Program Manager, Payer	<ul style="list-style-type: none"> 1. Healthier population 2. Lower costs of care 3. Helps to move various parties forward toward meaningful exchange of HIE, including e-LTSS data 4. Provide access to medical history for better diagnosis 5. Improved health management (shared lab results) 6. Improved care coordination 7. Available in emergency situations 8. Captures data outside of the medical office (e.g., exercise, over the counter drugs etc.) 9. Lower costs of care 10. Improved data sharing and analytics leading to better allocation of scarce resources 11. Ensures beneficiaries can see information about services received from public pay sources, helping to eliminate duplication and identify possible errors in their records, as well as recognizing trends in care
Federal Government	Funder, Policy Maker, Payer	<ul style="list-style-type: none"> 1. Healthier population 2. Lower costs

Stakeholder	Role	Value to the Stakeholder
		<ol style="list-style-type: none"> 3. Helps to move various parties forward toward meaningful exchange of HIE, including e-LTSS data 4. Provide access to medical history for better diagnosis 5. Improved health management (shared lab results) 6. Improved care coordination 7. Available in emergency situations 8. Captures data outside of the medical office (e.g., exercise, over the counter drugs etc.). 9. Lower costs of care 10. Ensures beneficiaries can see information about services received from public pay sources, helping to eliminate duplication and identify possible errors in their records, as well as recognizing trends in care

2.7 Project Scope

The scope of this business requirements document (BRD) is for the PHR for LTSS Demonstration. The PHR for LTSS Demo project is focused on producing a secure, web-based PHR system that will allow beneficiaries/legal representatives of Medical Assistance (MA) funded LTSS who are served by Collaborative members to access information about their services, enter information about themselves online (e.g., notes, diary entries or other functions that may be native to the PHR - this does not include making edits to DHS data), and securely share access to that information with others of their choosing.

The long term vision of the PHR for LTSS is to align with the DHS vision for integrated, client-centric service delivery across all DHS programs, as envisioned in the Enterprise Systems Modernization strategy. To the greatest extent possible or practical, this demonstration project is intended to put in place a demonstration PHR implementation for MA clients of LTSS that has the potential to be expanded across the state and possibly to include all DHS clients across all program areas.

The demonstration project represents an opportunity to implement a demonstration on a very small scale, and to learn from the demonstration:

- Whether the benefits of the PHR to beneficiaries that we expect are actually realized (i.e., the demonstration will help confirm and identify benefits to beneficiaries) as well as to lead agencies and service providers who are involved in the demonstration
- What would be required from a technology standpoint to effectively operate and expand the PHR
- What would be required from a privacy and security standpoint to expand the PHR
- What would be required to operate a sustainable PHR on a larger scale

2.7.1 Scope Accountability

Responsibility for demonstrating the PHR system described in this Business Requirements Document and appended Detailed Requirements Workbook will be shared by:

- **MN DHS PHR for LTSS Demo (State) Project Staff**, who will provide overall direction for the project and will ensure that the PHR is delivered within applicable cost, schedule, scope and quality constraints.
- **MN.IT @ DHS Staff**, who will perform the following tasks:
 1. Identify applicable data from DHS systems that needs to be provided to beneficiaries/legal representatives through the PHR.
 2. Ensure that the data from existing DHS systems is accurately characterized, aggregated and securely published out of DHS systems to be displayed in the Collaborative PHR by developing, testing and deploying the tools described in detail in the system diagrams and detailed business requirements documentation.
 3. Ensure that the aggregator (and related tools) is functioning properly by performing regular quality checks.
 4. Work closely with State and Collaborative staff to ensure secure, accurate, timely integration of data from DHS systems into the PHR as described in the attached detailed requirements documentation.
 5. Provide support to State and Collaborative staff to resolve issues that may arise with data quality, security or frequency throughout the life of the demonstration.
- **PHR Community Collaboratives**, which will perform the following tasks:
 1. Develop, test and deploy the necessary modifications to an existing Personal Health Record/Patient Portal for beneficiaries of MA waiver services.
 2. The Collaborative may choose from one of the following options for obtaining a Personal Health Record system:
 - a. One or more members has an existing contract with a vendor of an electronic health record (EHR) system certified by the Office of the National Coordinator for [Health Information Technology Certification Program](#) or [MN state "Qualified" EHR](#) with PHR functionality which could be modified and used for this project, or
 - b. The Collaborative or one or more members of the Collaborative has an existing contract with a [Minnesota State-Certified Health Information Exchange Service Provider \(HIESP\)](#) which has PHR functionality which could be modified and used for this project, or
 - c. The Collaborative will establish a contract with a vendor of a PHR product which can be modified and used for this project. If the Collaborative chooses this option, selection of the PHR vendor is subject to approval by the State.
 3. In collaboration with the State, develop, test and deploy the required modifications to a secure, web-based Personal Health Record (PHR) system to ensure that it meets the requirements set forth in this Business Requirements Document and Detailed Business Requirements Spreadsheets ([Appendix](#)).
 4. Work closely with State and MN.IT @ DHS staff to ensure secure, accurate, timely integration of data from DHS systems into the PHR as described in this Business Requirements Document and Detailed Business Requirements Spreadsheets ([Appendix](#)).

5. Develop and/or administer processes and policies to ensure privacy and consent safeguards are in place for the PHR to comply with the Health Insurance Portability Accountability Act (HIPAA), 45 CFR section 164.501, Health Insurance Portability Accountability Act (HIPAA) Privacy and Security Rule added in 2000, Health Insurance Portability Accountability Act (HIPAA) Omnibus Final Rule added in 2013, [Minnesota Health Records Act](#), Title 38 Section 7332 Protections Confidentiality of Certain Medical Records and [MN Government Data Practices Act](#) regulations. Process and policy documents must meet the criteria in section II.B.2.c of the PHR Community Collaborative RFP.
 6. Participate in the DHS Security Lifecycle Management process, including having the Collaborative's contracted PHR vendor(s) complete the "MN Department of Human Services Vendor Security Questionnaire" as required by the State.
 7. Ensure that all required security practices are followed throughout the course of the contract.
 8. Recruit LTSS beneficiaries/legal representatives served by Collaborative members, as well as caregivers, lead agency case managers, providers and other relevant users to participate in focus groups, usability testing, beta testing and use of the PHR in production. The Collaborative will work with State staff and/or consultants to ensure that beneficiary engagement is planned, communicated and executed so that the project results in a genuinely person-centered experience.
 9. Track/document how the information is used and by whom to make adjustments during implementation and evaluate the utility of the tool.
 10. Develop and/or alter existing video and text-based training materials for using the PHR. Materials must meet all criteria in section II.B.2.b. of the PHR Community Collaborative RFP.
 11. Provide telephone and web-based user support during regular business hours following deployment of Release #1 in the production environment until the end of the demonstration. This support includes assistance with authentication, training in use of the system, troubleshooting and ongoing technical support.
- See **Figure 1** below for an overview of the responsibilities of State Project Staff, MN.IT @ DHS Staff, and the Collaborative.

PHR Solution Definition & Development Process

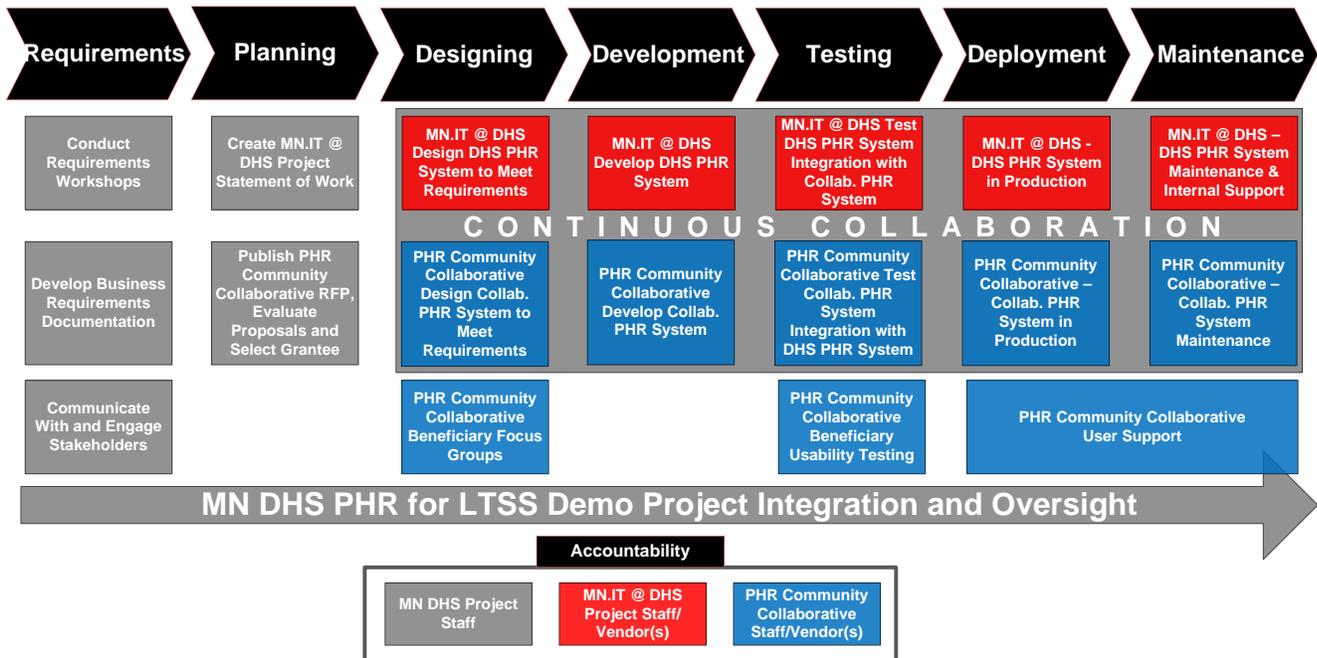


Figure 1

2.7.2 In Scope

The demonstration project scope is intended to implement and operate a demonstration PHR solution, as illustrated in the “RFP #2” timeline depicted in **Figure 2** below (or as modified during contracting). The functionality of each release is thoroughly identified in the detailed requirements in [Section 4](#) of this Business Requirements Document.

In general terms, the PHR will be moved to production according to a timeline to be agreed upon by the PHR Collaborative and the State.

- **Release #1** (Version 1.1.0, tentative production date to be determined, but no later than 4/1/2017) will provide the following general functionality:
 1. Electronic view of DHS communications – users will be able to access and share some information that is currently generated by DHS systems and sent via US mail within the PHR. Data from DHS systems that is displayed in the PHR will be “pushed” from those systems and will be read-only. Nothing that is entered by users of the PHR will be used to update DHS systems.
 2. Case manager name and contact information – users will be able to access and share case manager name and contact information within the PHR.

3. Text /Email notifications (e.g., rules based messaging service) – Users will receive automated notifications via text to their cell phone and/or email generated by the PHR system when information from DHS is updated in their PHR.
4. Discrete sharing of PHR information – users will have granular control of access permissions, allowing them to share all or only selected portions of their PHR with users to whom they grant the right to access their PHR.
5. Data entry – Users will be able to enter/update/delete information about themselves (e.g., notes, diary entries or other functions that may be native to the PHR - this does not include making edits to DHS data) that can then be shared with other users at the discretion of the beneficiary or their legal representative.
6. Electronic view of information – Users will be able to access and share read-only versions of Service Plans and Explanations of Benefits.
7. Additional functionality (as feasible) – Users will be able to share additional information, including current lists of medications, allergies, problems, etc. Respondents should indicate in their proposals whether the additional information listed here could be securely shared through their PHR solution, as well as whether there are additional types of information not listed that could be shared in the PHR.

The State and the Collaborative will agree on the specific service provider data sources, and may mutually agree to shift the availability of features in the interest of achieving the most optimum solution within the time and budget constraints.

The State and the Collaborative are expected to operate and support their respective components of the PHR solution for the duration of the grant period.

It is possible that sub-releases or maintenance releases may be required and will be mutually agreed upon by the State and the Collaborative.

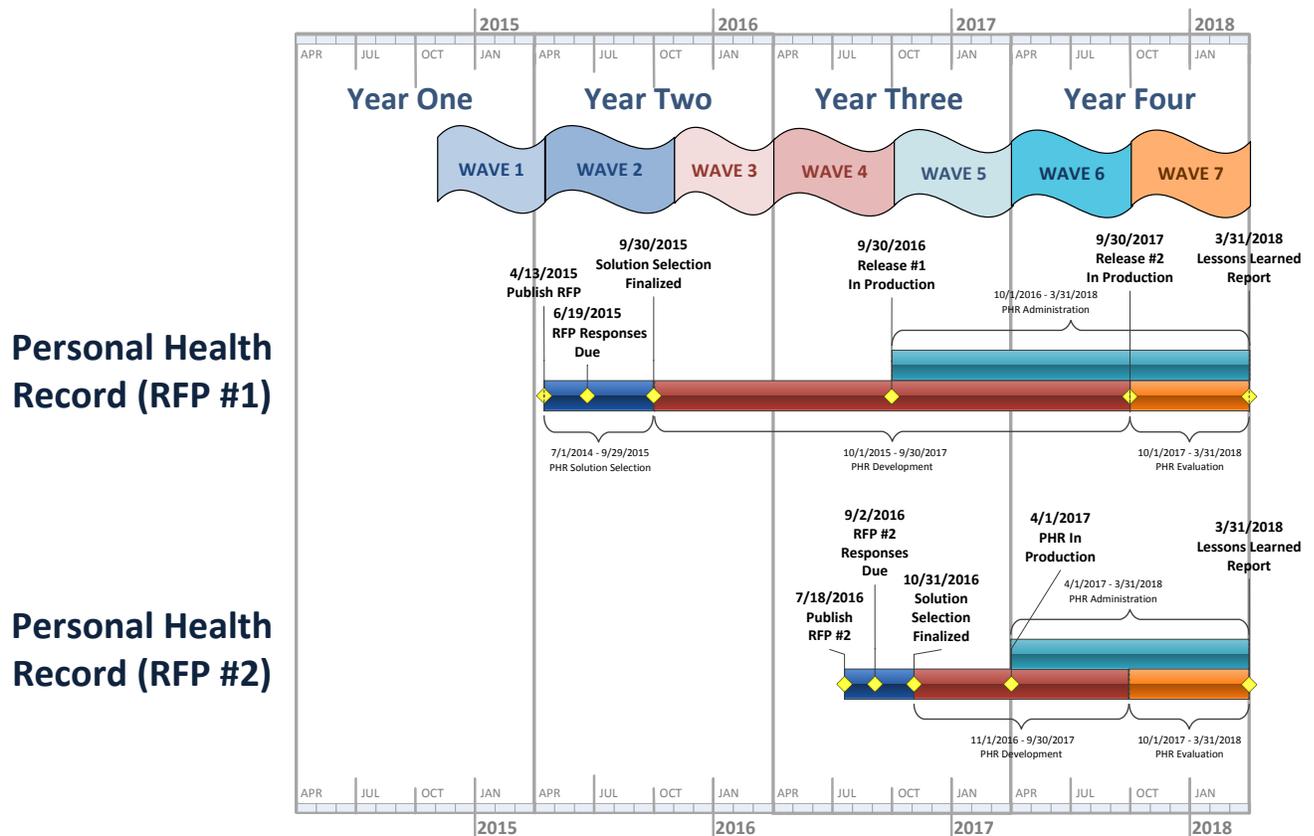


Figure 2

Functional Scope:

The functional scope of the solution is defined in [Section 4.1](#).

Information Scope:

The scope of the information to be aggregated and made accessible via the PHR is defined in [Section 4.4](#).

Geographic Scope:

The demonstration is expected to be geographically limited to one or more counties per Collaborative as defined by the State and the Collaborative.

Application Scope:

The scope of the application to be provided includes all components identified in [Section 4.3](#).

Technical Scope:

The solution must include all technologies required to meet the full set of requirements specified in [Section 4](#).

Organizational Scope:

The project will involve collaboration between:

- State Project staff responsible for the overall PHR for LTSS Demo project,
- MN.IT @ DHS for State IT support (and any service providers they need to meet their responsibilities), and
- The Collaborative (and any IT solution service providers they need to meet their responsibilities).

End User Scope:

The solution needs to support the use of the PHR by beneficiaries/legal representatives and others to whom they may grant access, applicable Case Managers, LTSS Providers and System Administrators, as defined in [Section 4.1](#) and [Section 4.2](#).

2.7.3 Out of Scope

The demonstration project scope is intended to implement and operate a demonstration PHR solution, as defined in the previous section, and no further major releases. It does not include support for operations beyond the grant period. It does not include rollout of the solution beyond the functional, informational, geographic, and organizational or end user scope as defined above.

However, should the demonstration be considered successful, DHS will want a Collaborative partner who is willing and able to extend the duration of the demonstration, and expand the scope potentially through additional releases that would be subject to appropriate financial support and contractual negotiations.

It is important to note that the PHR is not intended to replace any existing business processes or existing system functionality. The PHR will provide an alternate means of access to information already accessed and used through existing communications channels and systems, and is planned to exist only for the duration of the grant period.

2.8 Assumptions, Dependencies, and Constraints

2.8.1 Assumptions

It is assumed that the project can be carried out in the timeframe required by the TEFT Grant, and within the budget allocated.

[Section 4](#) defines all of the requirements identified to date that need to be addressed to implement and operate the PHR Demonstration for the period specified in the Grant. Section 4 further specifies who is expected to be accountable for delivering each requirement, principally either MN.IT @ DHS or the Collaborative. It is assumed that MN.IT @ DHS will manage any vendors or service providers it may need to deliver the requirements for which it is responsible, and similarly the Collaborative will manage any vendors or service providers it may need to deliver the requirements for which it is responsible.

The requirements specified in this document represent the definition of what is required and what is believed to be achievable at this point in time. It is recognized that more detailed

specifications will be developed as part of the next phases of design and implementation, and the scope of requirements is likely to be refined and may be changed as agreed upon by the participating parties.

2.8.2 Dependencies

No specific project dependencies have been identified at this time. Although the intent of the Demonstration project is to align with DHS Enterprise Modernization strategies, plans and architectures, and leverage these to the greatest extent possible, the specified TEFT grant timelines do not permit delay of the demonstration to wait for DHS modernization projects to be completed. Therefore, the Demonstration will leverage architectures, technologies and solutions that are available when needed to meet the schedule, and will leverage legacy systems solutions and technologies that are already in place when Enterprise Modernization solutions are not available within the TEFT grant timeline.

2.8.3 Constraints

The key constraints identified to date include:

- The objectives, requirements, and deliverables specified in the Grant must be addressed.
- The budget and schedule limitations of the Grant must be complied with.
- The PHR Demonstration must adhere to all relevant DHS privacy policies, state and federal privacy legislation – listed in [Section 4](#).
- The PHR demonstration must be carried out in accordance with DHS legal policies.

3. PROJECT OVERVIEW

The project team leveraged the State of Minnesota Department of Human Services Enterprise Systems Modernization (ESM) plan to align this effort with other MN.IT @ DHS related initiatives and the overall IT strategy. The ESM plan consists of a broad range of requirements and architectures, which represent the target which will guide DHS’s implementation of solutions over the next several years to realize its Integrated Human Service Delivery vision for the citizens of Minnesota, across all program areas.

The ESM plan contains a very high level Target Operating Model for DHS integrated service delivery, to support the flowing high level vision:

“A people-centered human services delivery system in which policy, people, processes, and technologies are aligned to serve the DHS mission”

- “DHS systems will become more integrated, aligned and adaptive to change.
- “Program and administrative efficiencies and effectiveness will increase.
- “Integrated technologies and data bases will better support information sharing and provide a holistic view of clients.
- “Staff become [sic] more knowledgeable about the programs and services available to citizens, and are able to apply their skills to do rewarding work.”

As noted above, the demonstration project is intended to align with Enterprise Systems Modernization to the extent it is applicable and practical within the constraints of the grant. The PHR for LTSS Demo project scope is focused on supporting only a very specific program area, and will be limited to specific functionality, geography, and organizational involvement as described above and in the following sections.

3.1 Current Process

A Personal Health Record system does not currently exist that performs the requirements indicated in this business requirements document.

The PHR Demonstration essentially represents a new channel for selected beneficiaries to access information already collected and provided by existing DHS processes and systems. It will not replace any existing channels, processes or systems, since it is being extended only to a limited subset of beneficiaries for a limited time period. In other words, beneficiaries who currently receive notifications via regular mail will continue to receive notifications through regular mail, even if those notifications are also available via the PHR. The existing channels, processes and systems will continue to be considered the authoritative channels, processes and systems. The PHR will only represent an alternate channel, and part of the assessment of the demonstration will be to determine if it is in fact considered to be a viable, desirable, reliable, convenient channel for beneficiaries to access information about the LTSS services they receive.

3.2 Proposed Process

The DHS Enterprise Systems Modernization Business Top Model was leveraged as part of this effort in order to identify the key business activities that could be related to use of a PHR. The intent of the DHS business model is to represent business functions and processes performed by DHS that are generalized across program areas to the greatest possible extent (i.e., the model is not program specific – most functions and processes apply to many, but not necessarily all program areas).

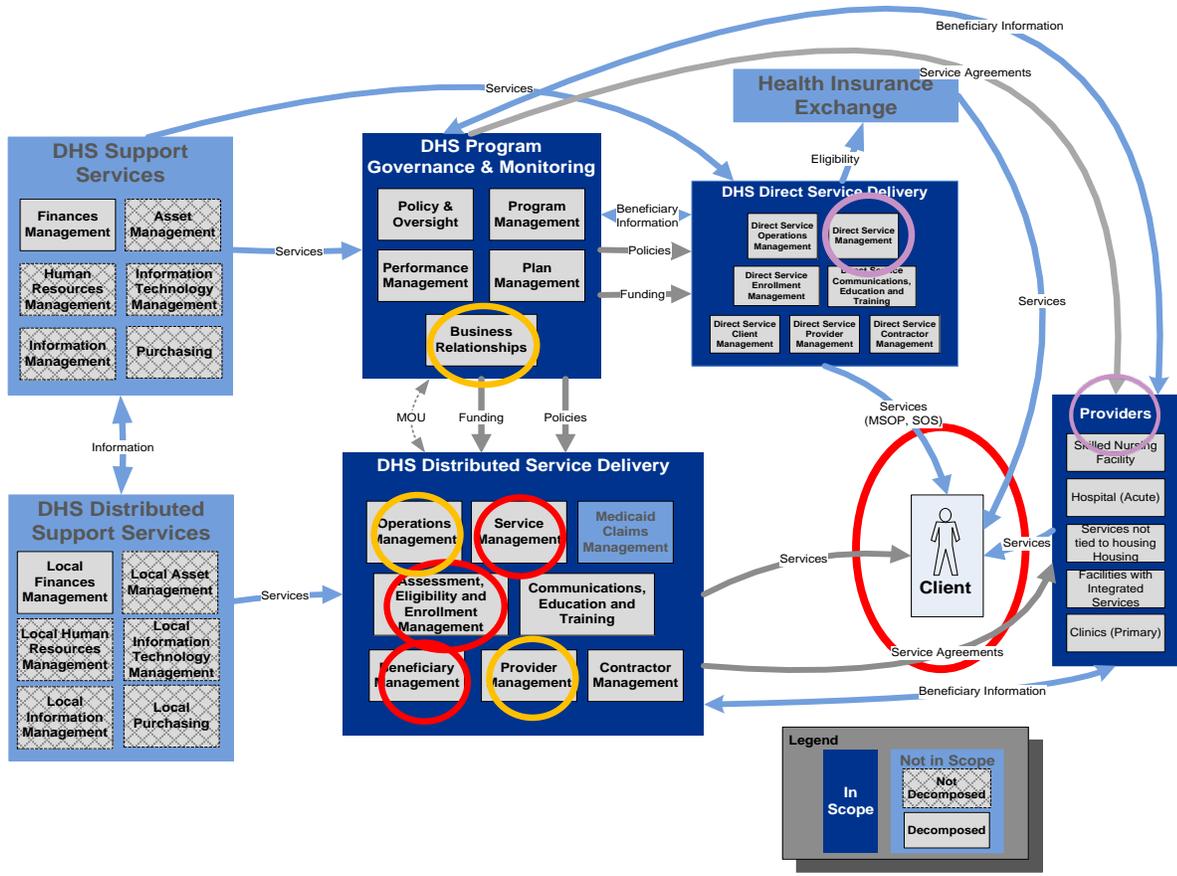


Figure 3

The diagram above (**Figure 3**) has been modified to highlight functions in which beneficiary information is captured and provided (red circles) and in which related provider information is captured (yellow circles). Note that we added high level processes carried out by Providers in which beneficiary information is captured or shared (these processes were considered out of scope for modernization).

This helped identify the types of parties who could be involved in the PHR demo – first and foremost, the beneficiaries/legal representatives and beneficiary-authorized users, and secondly, the Case Managers responsible for identification and application of appropriate services to meet the needs of the beneficiary.

As a result of this analysis, we identified the following major functions to be in scope for the PHR Demonstration:

- Beneficiary PHR Access and Use** – this represents the functions of the PHR that would be used by Beneficiaries/legal representatives - the main target user group of the PHR demonstration project. This functional area includes functions that would be used by designated beneficiaries of LTSS programs and their legal representatives, as well as other users authorized by the beneficiary to access their personal health records.

- **Case Manager and LTSS Provider PHR Access and Use** – this represents PHR functions that would be performed by designated, authorized LTSS program case managers who would be able to view PHR data through the system. Typically, these users would be LTSS case managers (members of lead agencies). Additionally, select staff of LTSS Providers could also access information about beneficiaries (with appropriate permissions) through the system. Giving these users access to some or all of the aggregated data in the PHR (as determined by the beneficiary) may enable them to provide better service to the beneficiary.
- **PHR Management, Operations, and Administration** – this functional area addresses the functions that need to be performed to administer and operate the PHR service by ensuring appropriate security, access, and information management, as well as the ability to report on the usage and effectiveness of the PHR service.

These functions are elaborated in [Section 4.1](#).

4. BUSINESS REQUIREMENTS

4.1 Functional Requirements

Functional requirements capture and specify the intended behavior of the PHR. They define how the key users interact with the PHR, as well as identifying key automated business functions. The PHR functional requirements were separated into three functional areas (as defined in the previous section) to define the specific use cases for the PHR:

- Beneficiary PHR Access and Use
- Case Manager and LTSS Provider PHR Access and Use
- PHR Management, Operations, and Administration

4.1.1 PHR User Roles

The PHR Demonstration is intended to be operated and used by the following roles, as defined below. Each of the specific functional requirements identifies the specific roles expected to use the function (i.e., the role involved in the use case).

Roles	Description
Beneficiary	A designated beneficiary of LTSS programs.
Legal Representative	A legal representative designated for a specific beneficiary, as defined in MMIS. For the PHR, the legal representative has the same access rights as the beneficiary.
Beneficiary Authorized User	A user identified and authorized by the beneficiary to view part of all of their PHR.
Collaborative PHR System Administrator	A system administrator of the Collaborative PHR, responsible for designated system administration functions related to the PHR.
MN.IT @ DHS System Administrator	A system administrator for the MN.IT @ DHS Data Aggregator and DHS source systems, responsible for system administration of these functions.
Case Manager	An LTSS case manager specified in one or more DHS source systems (this may include a certified assessor who is acting in the role of case manager in some cases)
LTSS Provider Staff	Users identified by a Collaborative LTSS provider that serves the beneficiary authorized by the beneficiary to view all or part of their PHR.

4.1.2 Beneficiary PHR Access and Use – Functional Requirements

The processes depicted in the following diagram (**Figure 3**) illustrate the functional requirements for how beneficiaries and/or their legal representatives will use the PHR.

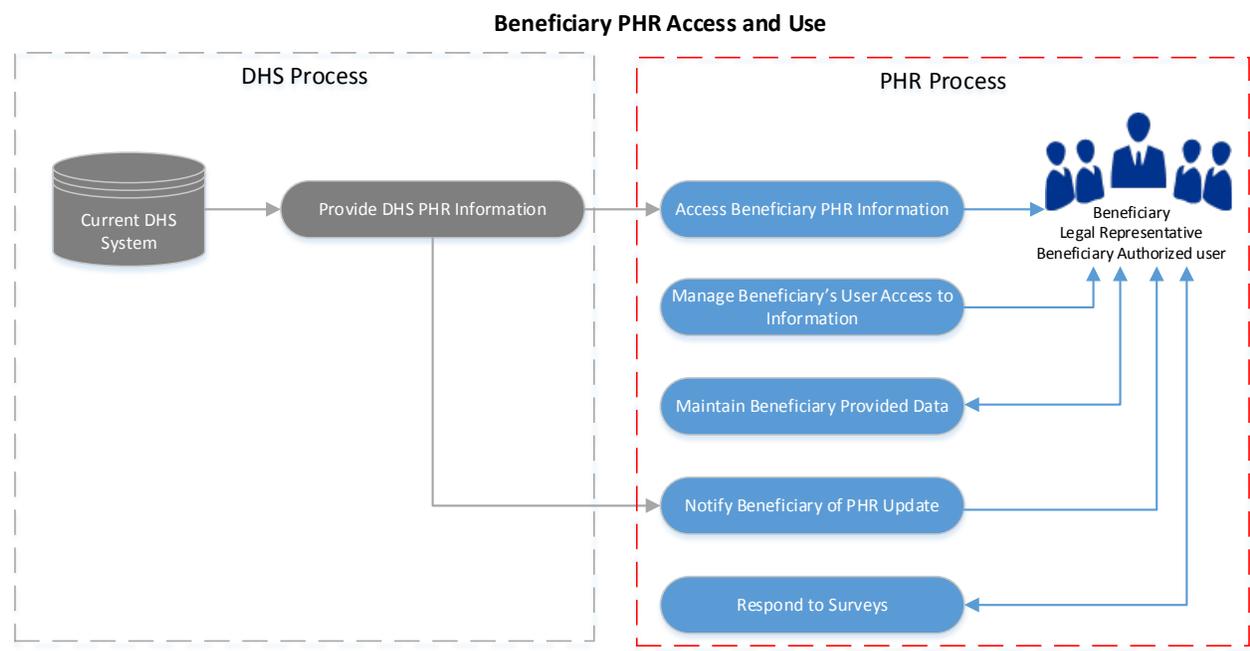


Figure 4

One or more Functional Requirements have been defined for each of the processes depicted above. The above functional requirements are found on the “FR – Beneficiary-Legal (BL)” spreadsheet in the appendix.

4.1.3 Case Manager and LTSS Provider PHR Access and Use – Functional Requirements

The processes depicted in the following diagram illustrate the functional requirements for how authorized Case Managers and Assessors will use the PHR.

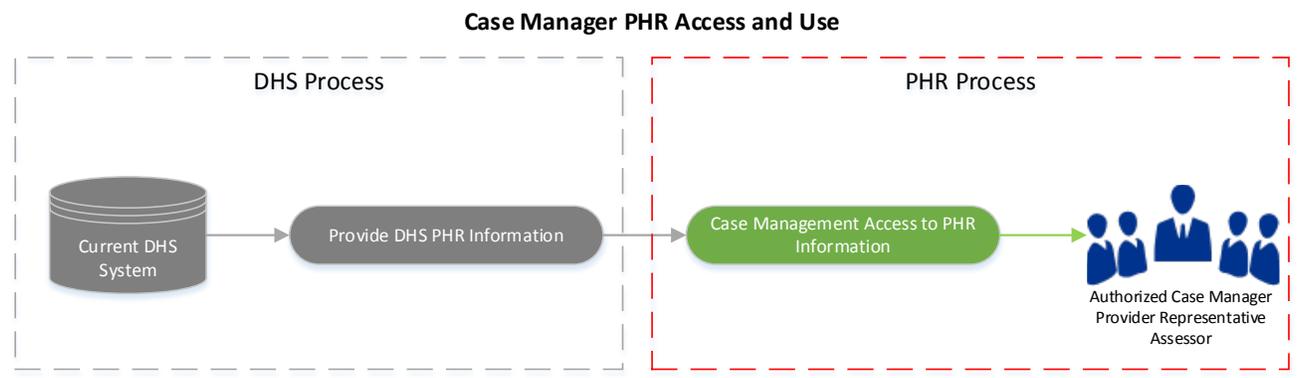


Figure 5

One or more Functional Requirements have been defined for each of the processes depicted above. The above functional requirements are found on the “FR – Case Manager (CM)” spreadsheet in the appendix.

4.1.4 PHR Management, Operations, and Administration – Functional Requirements

The processes depicted in the following diagram (**Figure 6**) illustrate the functional requirements for how the system administrator will access the PHR, including user tracking and registration management.

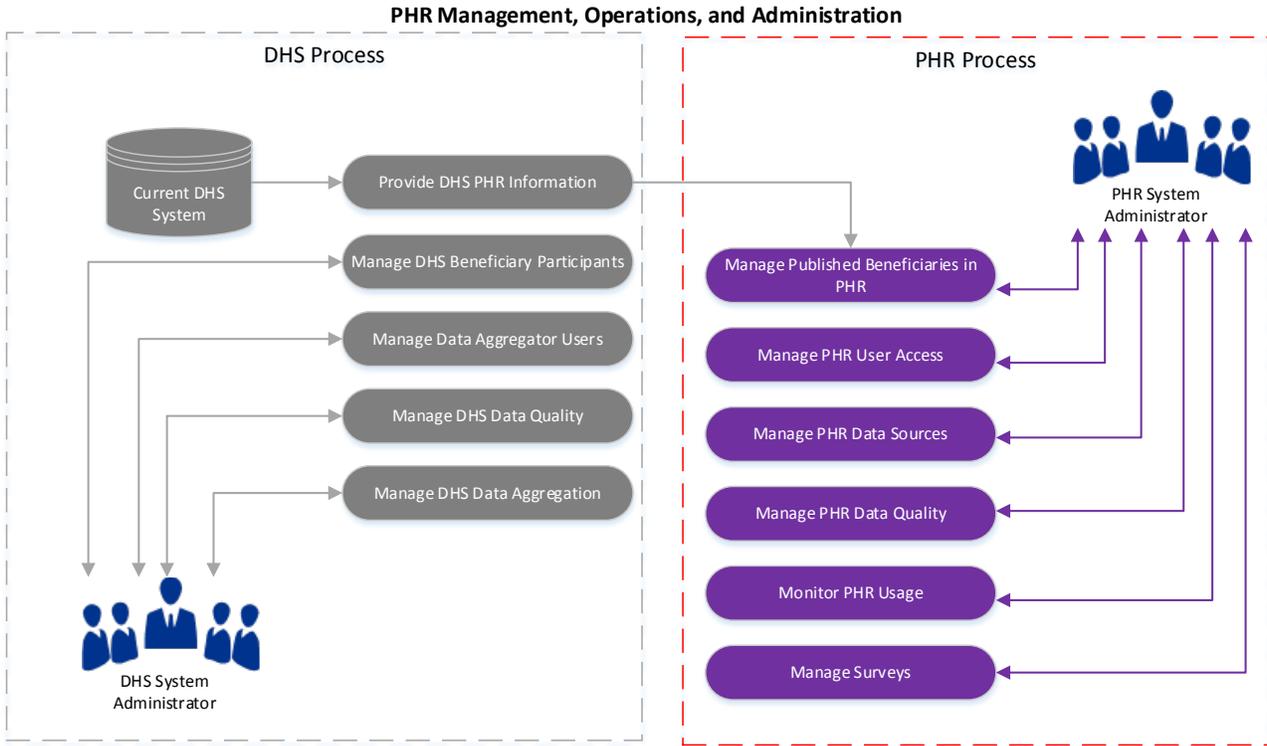


Figure 6

One or more Functional Requirements have been defined for each of the processes depicted above. The above functional requirements are found on the “FR – Administration (AD)” spreadsheet in the appendix.

4.2 User Experience Requirements

User experience requirements describe all of the business requirements associated with the user experience, including accessibility for people with disabilities, usability, ease of learning, task efficiency, ease of remembering, understandability, and aesthetics or attractiveness.

User experience guiding principles:

- [CMS Seven Conditions and Standards](#) - “The system architecture should utilize a user interface (UI) framework that deploys presentation components to allow for communication with disparate populations using different media formats such as web, email, mobile, and short message service (i.e., text messaging).”
- Accessible for users with disabilities, meeting or exceeding standards for accessibility as defined by the State of Minnesota’s [Accessibility Standard](#).
- User experience requirements include specific requirements for the solution itself, and also include requirements for user experience related services to be provided by the Collaborative.

User experience requirements have been grouped into three target user groups, which have different user experience requirements:

- Beneficiaries/legal representatives and other beneficiary authorized users,
- Case Managers and LTSS Providers, and
- System Administrators.

4.2.1 PHR User Experience Requirements for Beneficiaries and Legal Representatives

The user experience for beneficiaries and their legal representatives (as well as other users allowed by the beneficiary, if applicable) is a critical success factor for the PHR demonstration. It will be important that the PHR is easy for beneficiaries and their legal representatives in particular to use. The target groups for using the PHR are often elderly and/or disabled, so accessibility will be important, and the target group is more demanding than what would be considered average for publicly accessible user interfaces.

The user experience requirements for beneficiaries and legal representatives are found on the “UE Reqmts (BL)” spreadsheet in the appendix.

4.2.2 PHR User Experience Requirements for Case Managers and LTSS Providers

Case Managers and LTSS Providers will have a subset of functionality available to them relative to the beneficiaries and their legal representatives, and so the user experience requirements are less demanding.

The user experience requirements for Case Managers and LTSS Providers are found on the “UE Reqmts (CM)” spreadsheet in the appendix.

4.2.3 PHR User Experience Requirements for System Administrators

System Administrators generally have a different set of functions available to them and have less demanding user experience requirements.

The user experience requirements for System Administrators are found on the “UE Admin Req (AD)” spreadsheet in the appendix.

4.3 Target Architecture

4.3.1 Architecture Context

The following diagram (**Figure 7**) depicts the context for the PHR Demonstration Solution.

The PHR Solution is intended to aggregate data from DHS systems containing relevant beneficiary case management information for selected LTSS program beneficiaries. In Release #2, it may also aggregate selected clinical data from participating healthcare service providers.

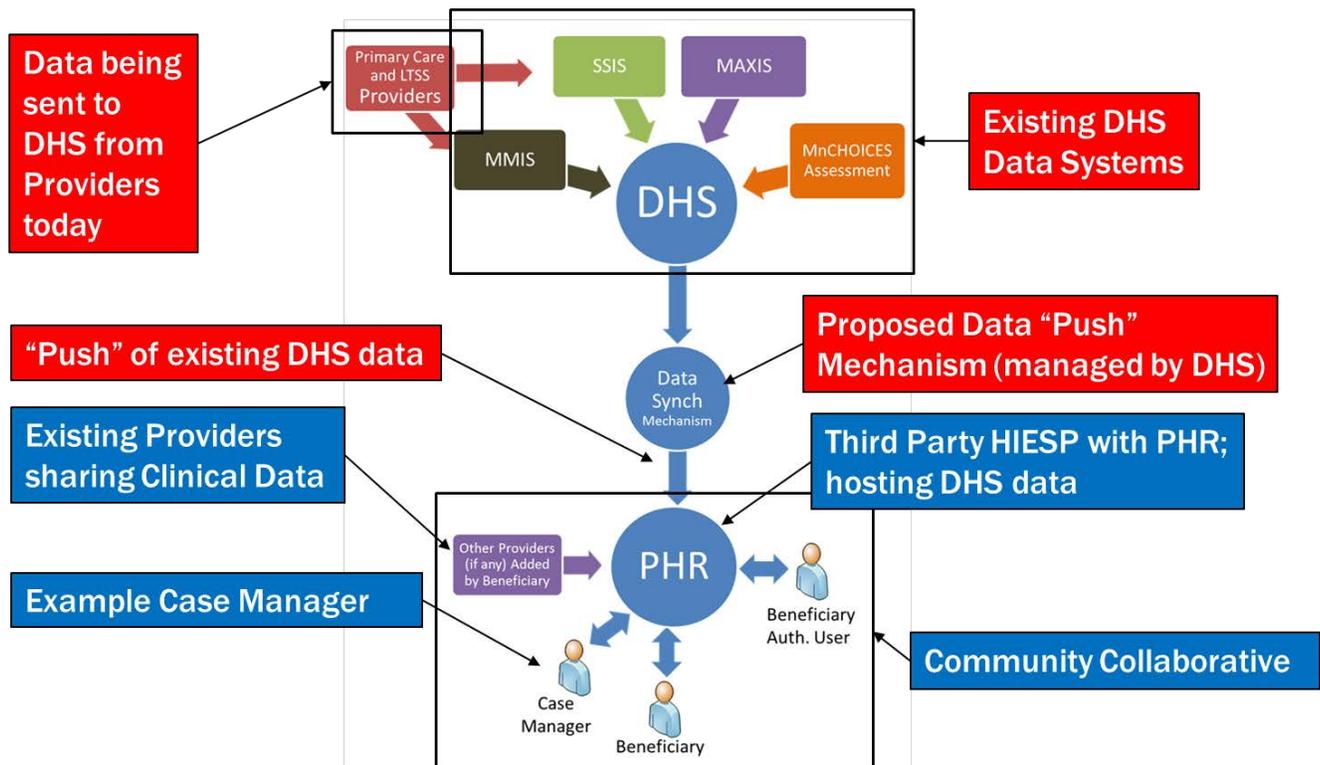


Figure 7

MN.IT @ DHS will be responsible for DHS source systems interfaces and the Data “Push” Mechanism (see red boxes). The Collaborative’s [Health Information Exchange Service Provider \(HIESP\)](#) is responsible for all components associated with the PHR itself (see blue boxes). Feeds from Other Provider source EHR systems are the responsibility of the external provider.

The following sections describe the individual components involved in the solution in greater detail.

4.3.2 Target Solution Architecture

Target Architecture Diagram for the PHR Solution (Figure 8):

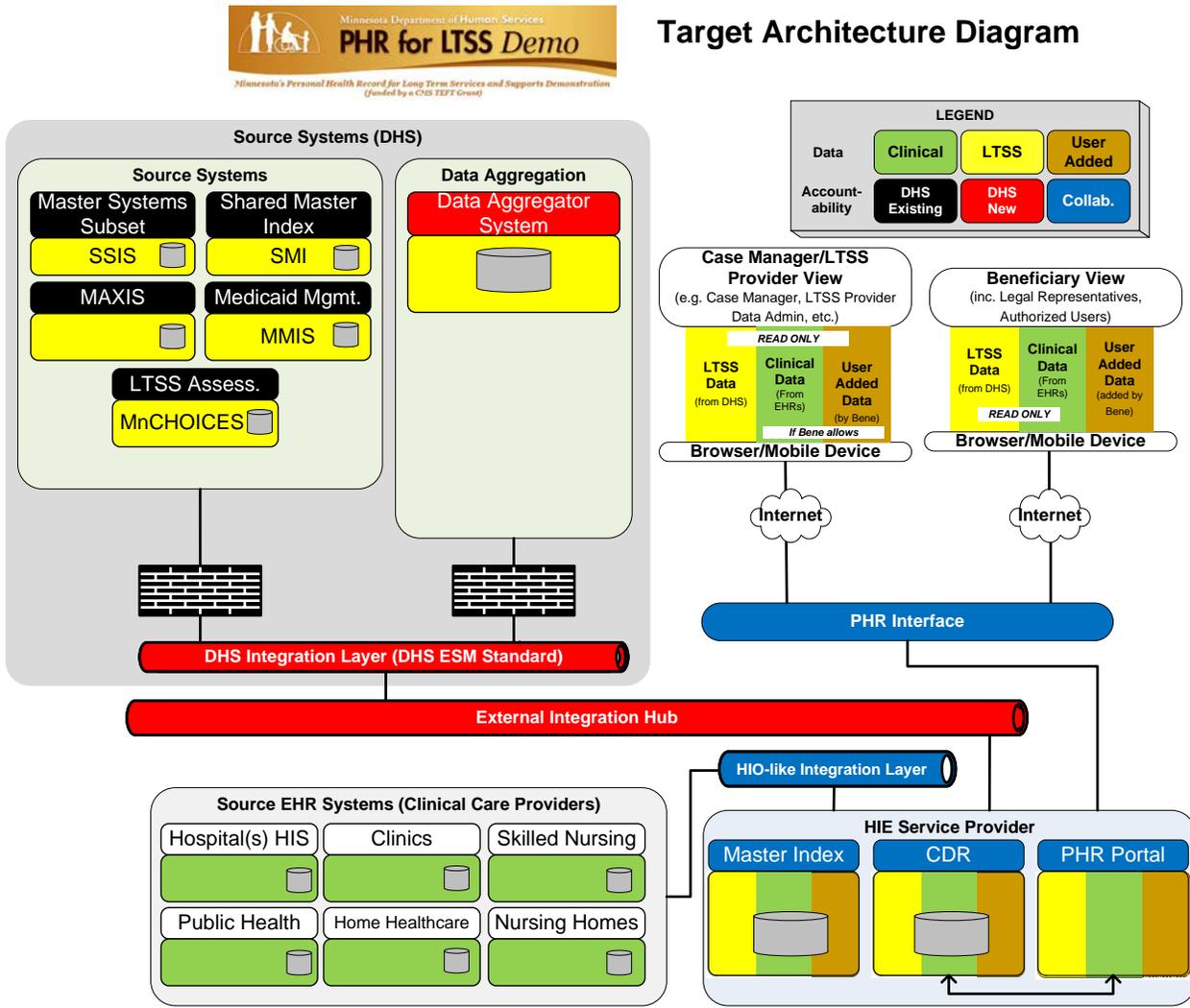


Figure 8

The PHR System is envisioned to have three main components in order to collect, consolidate and manage beneficiary data. The Collaborative may have different application component architecture than what is shown here, but it must be functionally equivalent.

HIO Integration Layer

A transport mechanism or Enterprise Service Bus (ESB) that will connect the PHR system with the data obtained by the Data Aggregator from source systems via the External Integrator Hub and the DHS Integration Layer. The HIO Integration layer should follow the same standard protocols and methods that are already in place for other PHR Systems. This compatibility will ensure, in future releases, the ability to integrate other external providers as part of the PHR solution.

The Collaborative is accountable for the design, setup and implementation of the HIO Layer. MN IT @ DHS will provide details on the mechanisms required to connect to the External Integration Hub and the mechanism to push data into the PHR system.

Clinical Data Repository (CDR)

The CDR is the component that stores and manages all data collected from the source systems, including DHS source systems and clinical (EHR) source systems. This component is considered the consolidation point for all of the beneficiary data collected from the Source Systems. No user in the PHR system will have the ability to edit data elements collected from source systems, or create new information, with the exception of some data elements, such as beneficiary notes (see the information requirements in the section below). With respect to data collected from source systems, the PHR system will only provide read-only access to the data contained in the CDR.

Any modification identified by a registered user has to be done to the source systems via the existing channels (e.g., via case managers, call center, etc.) and not through the PHR system. In other words, any changes which the Beneficiary may want to make to this data must be updated by contacting their case manager or other LTSS contact and requesting data updates to the source systems. The updates will be forwarded to the PHR from the source systems via the integration components.

In addition to consuming data from two main sources (DHS systems and external healthcare service provider EHR systems), the PHR will allow the beneficiaries to generate and manage their own data in the CDR. The CDR will also generate data required for PHR management, operations and administration purposes. For more details on the data types and subjects, please refer to the information requirements section of this document.

Beneficiary Master Index

This is the component that maintains a mapping of all the beneficiary identifiers collected from source systems and to which beneficiary they are associated – i.e., mapped to the Beneficiary ID used in the PHR. This mapping includes the traceability of every beneficiary back to the source systems (or data aggregator for DHS systems). Every time a source system pushes data to the PHR, the Master Index will match the source system ID to the PHR Beneficiary ID to ensure that records are indexed to the correct beneficiary.

4.3.3 PHR Infrastructure

The PHR System will be hosted/served outside the DHS Infrastructure. It is considered an external system with direct access to beneficiary data published to it. Once all security and privacy requirements are met for the PHR system (e.g., data residency, security, etc.), it is up to the Collaborative to decide the geographic location of the PHR system within the U.S. and which infrastructure technologies to be used to enable it. DHS has no preferred architectural guideline, principles or standards that will apply to the Collaborative outside of security constraints. DHS is allowing the Collaborative to use the most suitable deployment, implementation and operation of the PHR System.

4.3.4 Source Systems

The PHR will consume data from the following systems:

DHS Source Systems

Via a data aggregator component, the PHR will collect beneficiary information from the following DHS systems:

- Shared Master Index (SMI)
- MAXIS – DHS Medicaid financial eligibility system
- Social Services Information System (SSIS)
- LTSS Assessment (MnCHOICES)
- Medicaid Management Information System (MMIS)

DHS Data Aggregator

The data aggregator will be the central point of consolidation of DHS data. The Data Aggregator is accountable to provide the capacity and scalability to add more DHS source systems in the future as well as grow to include additional beneficiaries from other geographic areas of the state, and other programs, should the solution scope be expanded after the grant period. It will need to maintain the same performance levels to serve data to the PHR. The aggregator will need to maintain a cross-reference of Beneficiary ID's from each of the source systems to the unique beneficiary ID within the Data Aggregator. The PHR system will not have direct access to DHS systems; it will only consume data published from the data aggregator. This is a restriction rather than a technical limitation.

DHS Integration Layer

The DHS integration layer is the internal DHS Enterprise Service Management standards that allow system components to interact within the DHS infrastructure. For the PHR Solution, this integration layer will not be visible and is out of scope. The Data Aggregator will use the DHS Integration Layer to collect data from DHS Source Systems and to interact with the External Integration Hub (See below) to push data into the PHR System.

DHS External Integrator Hub

The DHS External Integrator Hub provides the communication protocols, standards and mechanisms to connect any external systems with the DHS Integration Layer. This will be the source of communication between the Data Aggregator and the PHR System.

External Provider Source EHR Systems

Electronic Health Record (EHR) data from selected external providers may also be collected by the PHR System. Ideally, the PHR Provider will have established connections to the following types of healthcare provider EHR system components: hospitals, clinics, skilled nursing, public health, home healthcare and nursing homes. The PHR system should provide the flexibility and scalability to collect data from more external source systems in the future, beyond the grant period.

4.4 Information Requirements

The information requirements define the specific data items that must be included as part of the PHR. This is consolidated into a conceptual view of the data subject areas and key entities below (**Figure 9**).

PHR Conceptual Data Subject Areas and Key Entities

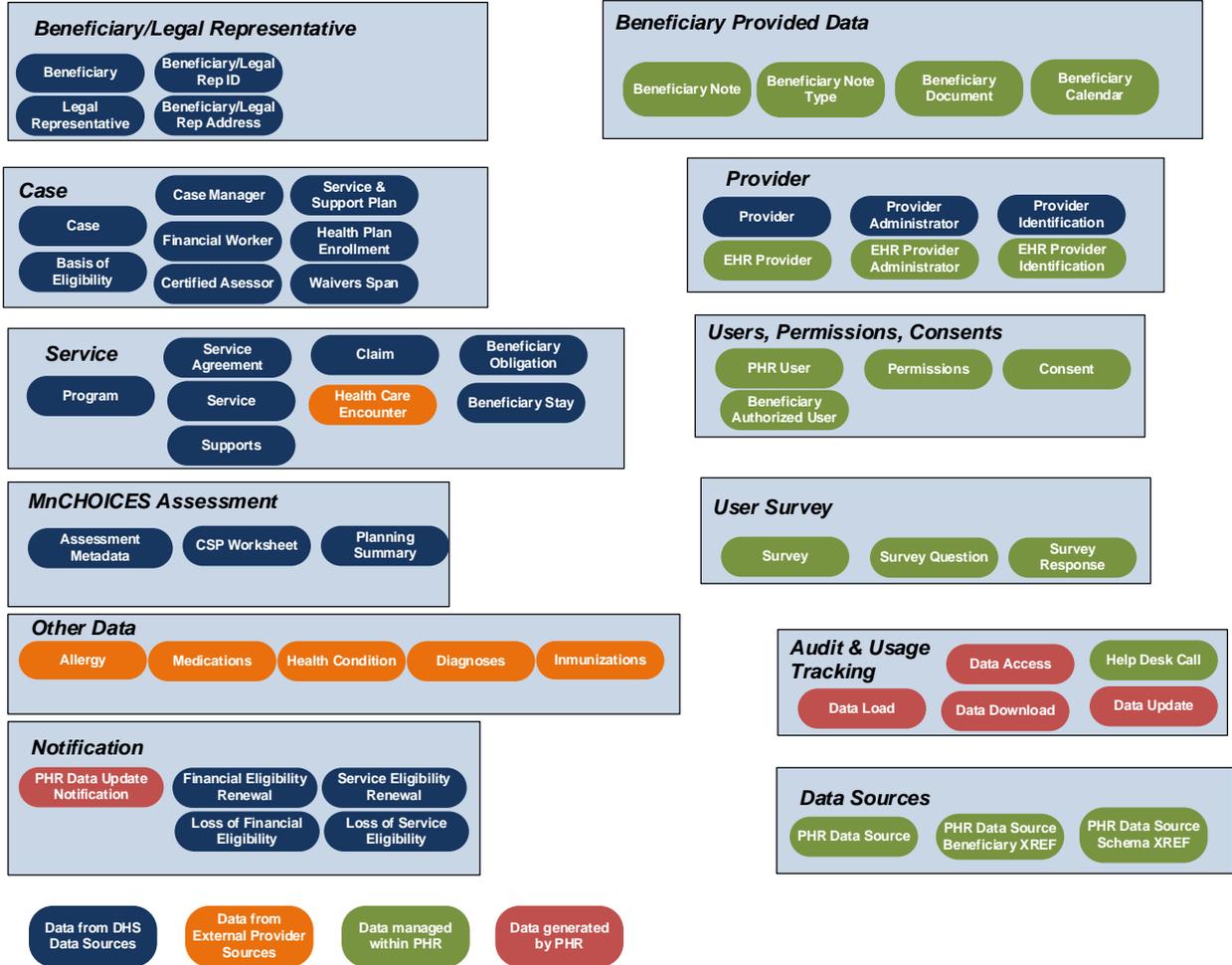


Figure 9

The PHR will consume data from the following subject areas identified:

Subject Areas

- Beneficiary/Legal Representative
- Case
- Service
- MnCHOICES Assessment
- Other Data
- Notification
- Beneficiary Provided Data
- Provider
- Users, Permissions, Consents

- User Survey
- Audit & Usage Tracking
- Data Sources

Data from DHS Data Sources

As defined in the PHR Architecture section, data from DHS Data sources will be published via a data aggregator component. The data aggregator will be the central point of consolidation of DHS data and main component of interaction with the PHR system. Key entities are depicted in blue in the model above which represent data from DHS Data Sources.

Data from External Provider Sources

As defined in the PHR Architecture section, data from External Provider Sources will be sourced via the HIO-Like Integration Layer. Key entities are depicted in the model above in orange which represents data from External Provider Sources.

Data Managed within PHR

Data managed within the PHR represents data that PHR users enter directly. This includes:

- Beneficiary Provided Data
- User Permissions and Consents (to be maintained by the PHR System Administrator)
- Help Desk Calls (to be recorded and tracked by the PHR System Administrator)
- Surveys and Survey Questions (to be maintained by the PHR System Administrator)
- Survey Responses (to be entered directly by Beneficiaries/Proxies)
- Registry of External Healthcare Service Providers and their EHR systems, including configuration information (mappings of their source system attributes to the PHR), used by the PHR to manage data loads from source systems

Key entities are depicted in green in the model above which represents data managed within the PHR.

Data generated by PHR

Data generated by the PHR System includes all logs of all data loaded, updated, accessed, and downloaded from the PHR, as well as a log of notifications to Beneficiaries (i.e. messages sent to beneficiaries notifying them of new data loaded into their PHR record). Key entities are depicted in red in the model above with data generated by the PHR.

Data Managed within the Data Aggregator

The diagram below (**Figure 10**) illustrates the data to be managed in the data aggregator.

PHR Conceptual Data Subject Areas and Key Entities – Stored in Data Aggregator

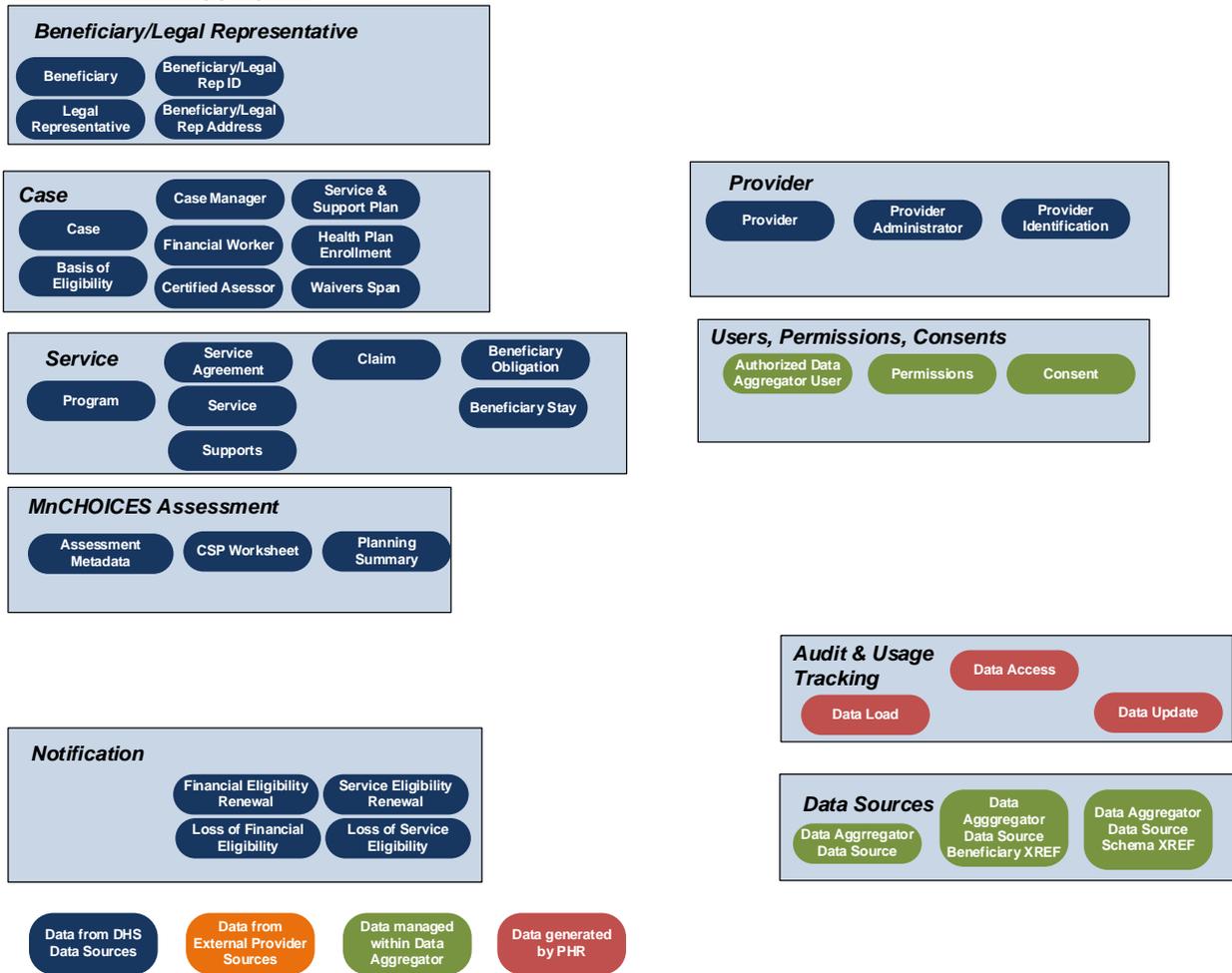


Figure 10

4.5 Integration Requirements

This section describes how the Integration of source data into the PHR is required to work.

Refer to the appendix for the spreadsheet containing more detailed definition of the interface requirements. They are found on the “NF – Interface Reqmts (IF)” spreadsheet.

PHR System Integration Overview

DHS source systems will not have a direct interface to the PHR system. All traffic and data generated from any DHS system will be consolidated inside the DHS perimeter. Each DHS System will match the beneficiaries that are included as part of the PHR System (Beneficiary will be selected based on pre-defined criteria) and are published from DHS source systems to the Data Aggregator component via the DHS Integration Layer. The Data Aggregator will push the aggregated data to the PHR System. Following the same principle, Source EHR Systems will push any clinical data that matches the beneficiary criteria and send it to the PHR System.

A more detailed description and flow of each one of the integration points can be found later in the document.

Please find below (**Figure 11**) the high level Integration architecture for the PHR System:

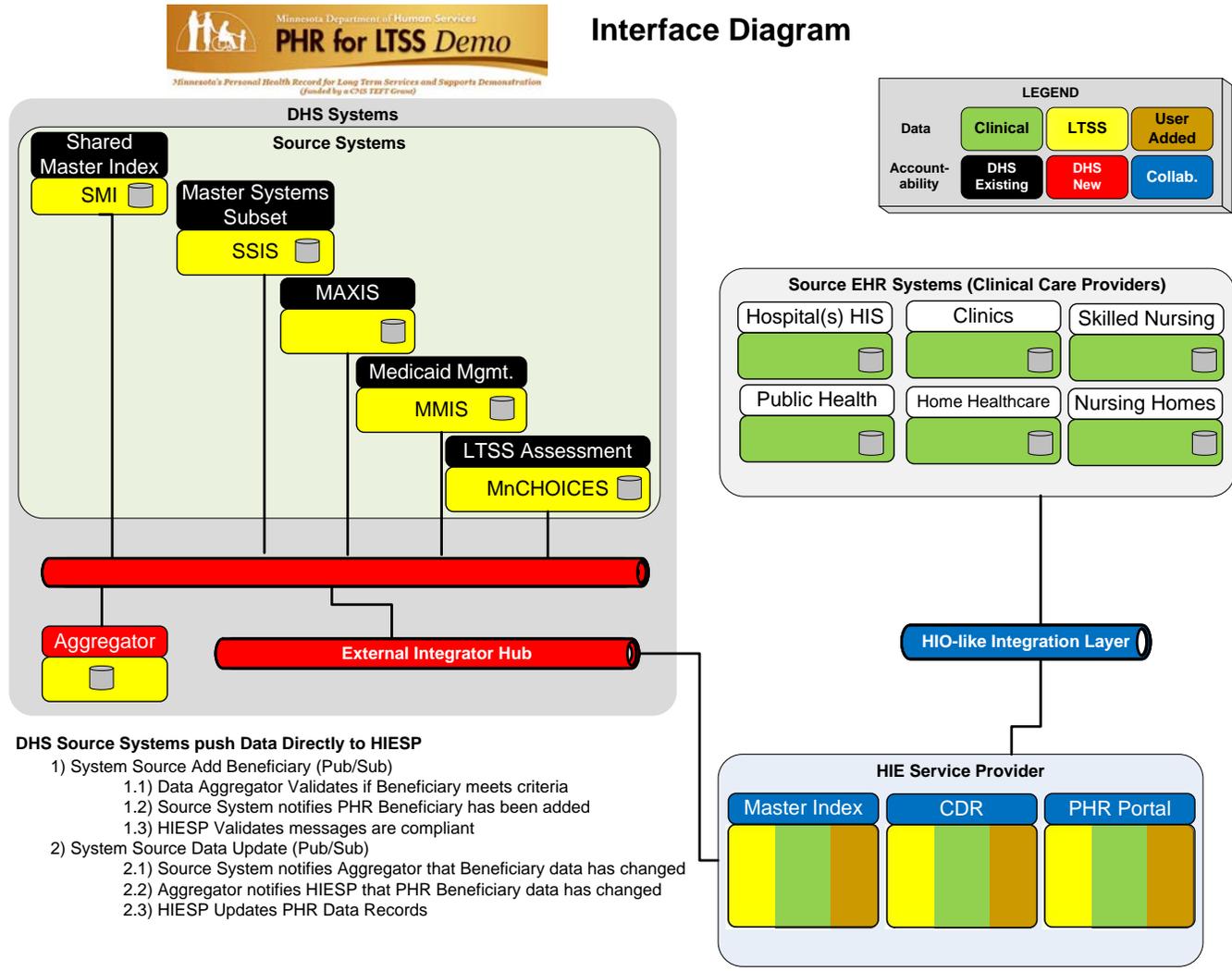


Figure 11

Integration of DHS Source Systems to PHR System

The diagram below (**Figure 12**) shows a detailed view of how the DHS systems are integrated and send data to the PHR system.

DHS to PHR Data Flow

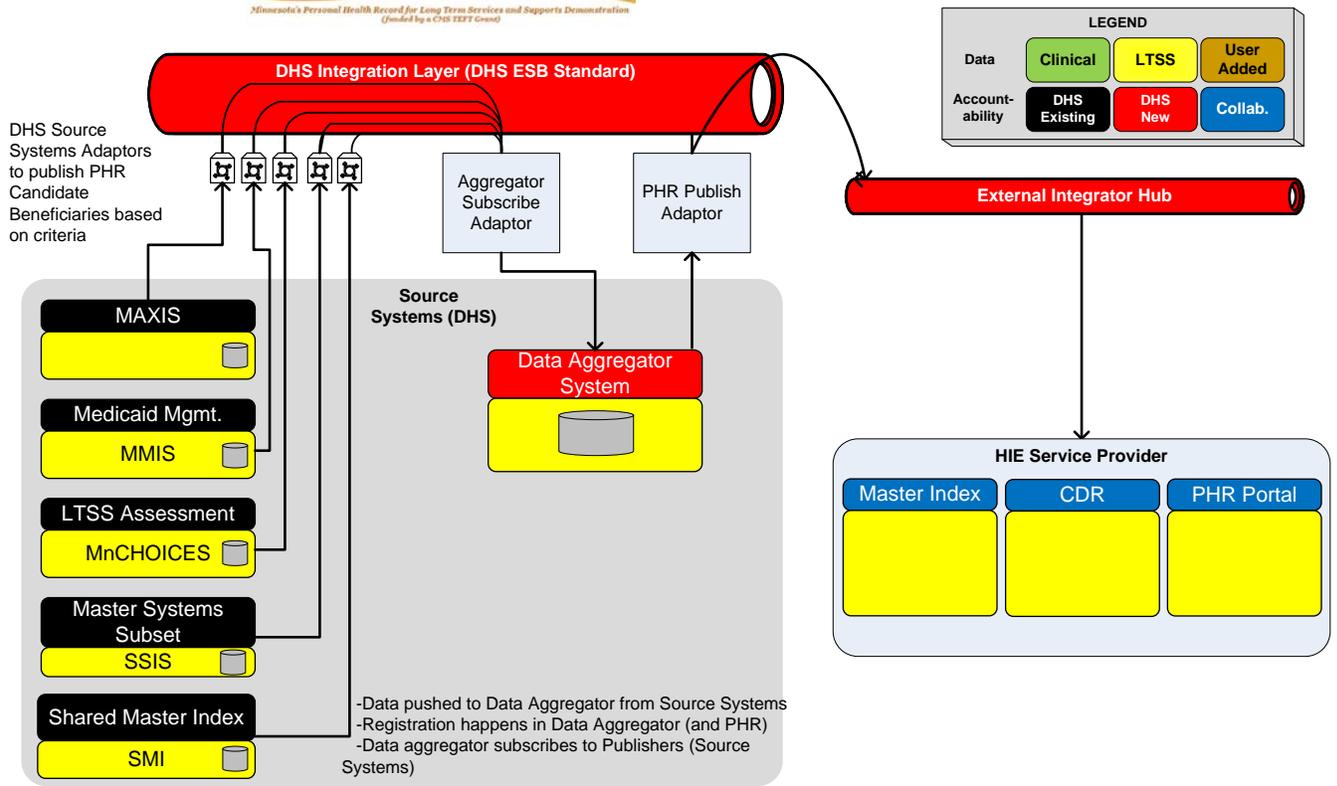


Figure 12

Via a series of adaptors, one for each DHS System, beneficiary data are pushed from the source systems to the data aggregator. The data aggregator component will be the data consolidation point for all information that DHS needs to send to the PHR System. The frequency at which each individual DHS system will send data to the data aggregator is open for each system owner to decide, as long as all updated data are pushed to the data aggregator before the daily push to the PHR system.

Once a day (details of the exact time for the push will be defined), the data aggregator will push all the data collected to the PHR System. The data aggregator mechanism will recognize the delta between the data already sent and the new uploaded data and will only send the new data elements identified for efficiency and performance purposes.

The existing version of the data aggregator has been designed to make use of secure web services provided by an existing PHR provider. The first web service provided by the PHR accepts content in an Admit, Discharge, and Transfer (ADT) format. The State's data aggregator is specifically using the ADT08 transaction to upload discrete data elements to the PHR provider's system. The second web service provided by the PHR provider is to Provide and Register Document Set-b Transactions – uploading .pdf files to the PHR to share information with the client. The State's expectation is that collaborative PHR Systems will be able to make use of these or similar transactions for integration of DHS data into their PHR. In addition, the State expects positive or negative confirmation from Web service calls. If

automated confirmation is not provided, the collaborative PHR needs to describe to the State how exceptions are managed across the provider's PHR interface.

Integration of HIE Service Providers to the PHR System

The following diagram (Figure 13) provides a view of the flow between source EHR Systems (Clinical Care Providers) and the PHR Systems:

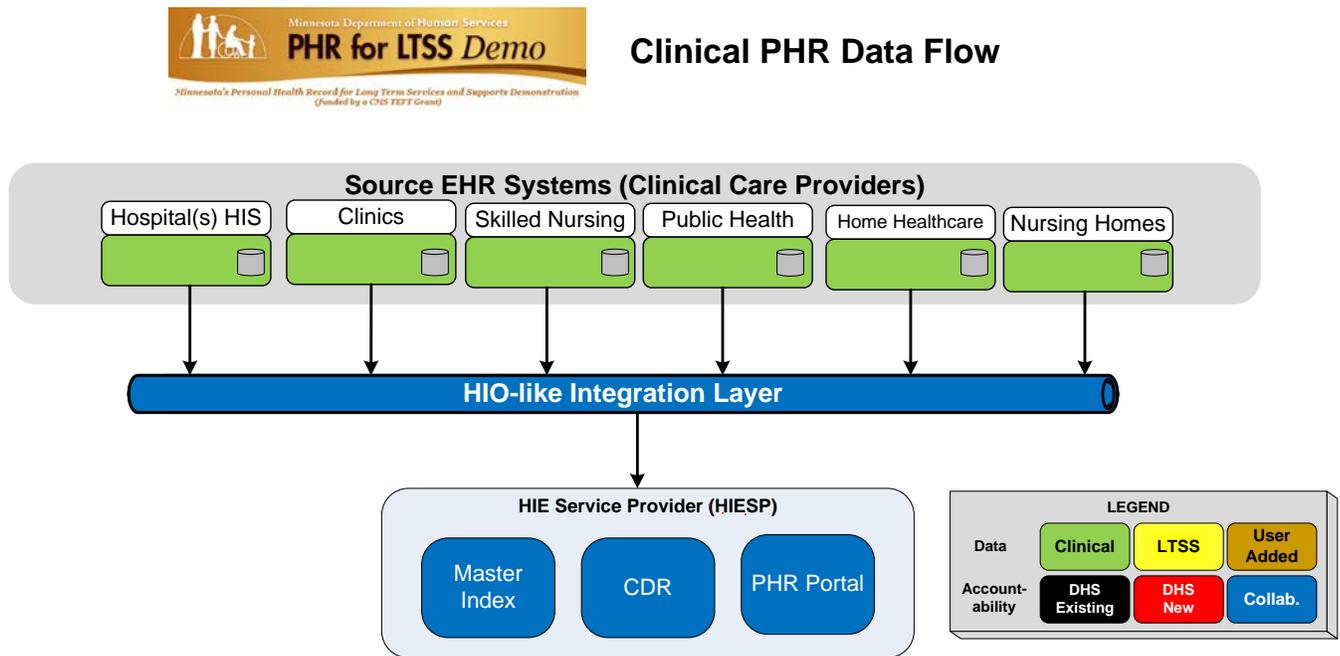


Figure 13

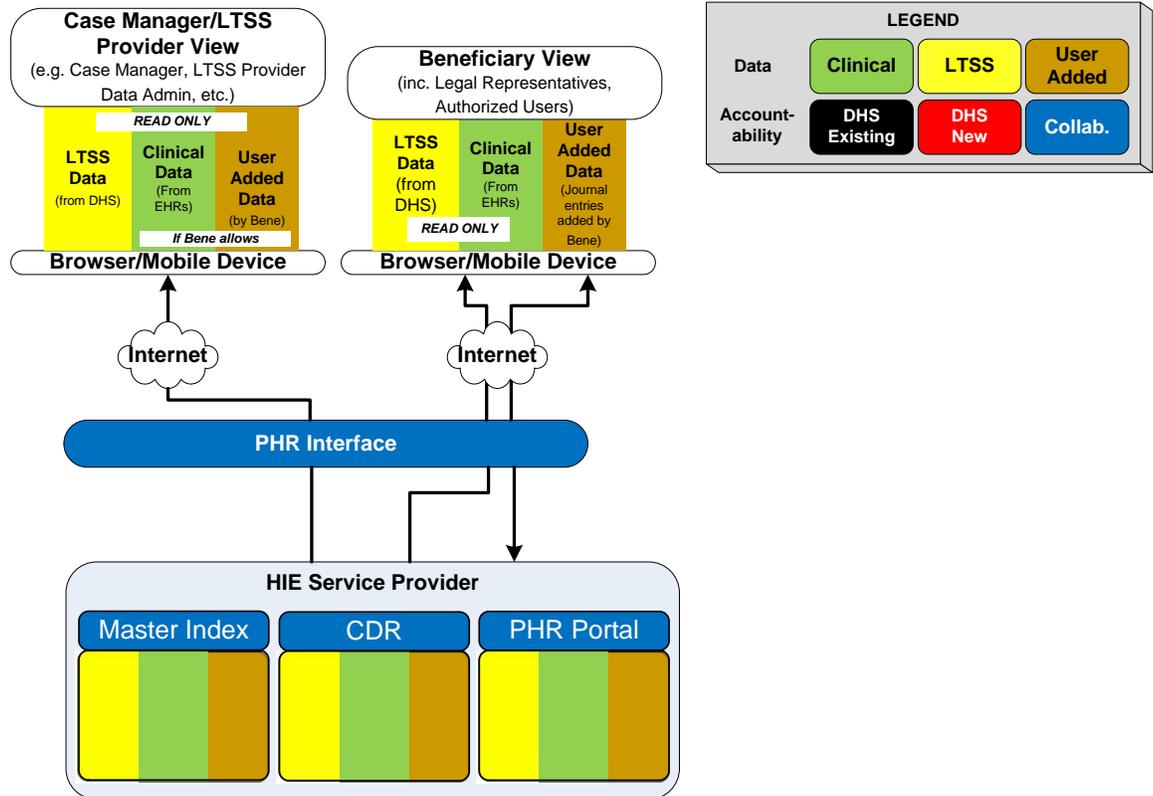
Access to the PHR System

The PHR System can only be accessed by a specific set of users from one of the following groups:

- Beneficiaries/Legal representatives and others to whom they grant access
- Case Managers and LTSS Providers
- System Administrators

Please find below (Figure 14) a representation of how users will access the PHR System:

User Data Flow



Case Manager/ LTSS Provider View

-Access only DHS portion of PHR data for all beneficiaries for whom they are Case Manager or LTSS Provider

Beneficiary View

- Access LTSS Data from DHS PHR data flow
- Access Clinical Data from Provider PHR Data flow
- Beneficiary can store notes and any other additional information in the User Added Data PHR section of the service
- Data added by the beneficiary will not be transmitted to DHS

Figure 14

Through a PHR Portal, each user will have access to the data previously collected by the PHR System. Each one of the user groups will have different capabilities and different access controls. For more details on capabilities and/or access controls, please refer to the security and privacy sections of this document.

4.6 Security Requirements

The security requirements for the PHR System describe all those functional and non-functional (technical) requirements that need to be addressed in order to achieve a comfortable level of security attributes of the PHR System. More than just a series of tool-specific requirements, these security requirements also cover organizational elements of the Collaborative such as

methods, operational model, standards and procedures that DHS would like to understand in more detail. Also the synchronization of activities between MN.IT @ DHS and the Collaborative is covered as part of the requirement list.

Refer to the appendix for the spreadsheet containing a more detailed definition of the security requirements. They are found on the “NF - Security Reqmts (SE)” spreadsheet.

4.7 Privacy Requirements

Typically, privacy requirements are a subset of the security requirements and they are included in the same list. However, due to the sensitivity and criticality of the information that the PHR Solution will manage, the State’s approach to present these requirements is to detach the security and privacy requirements. With this context in consideration, the Privacy requirements cover all the limitations, laws and regulations that need to be taken into account for the design and deployment of the PHR System.

Refer to the appendix for the spreadsheet containing a more detailed definition of the privacy requirements. They are found on the “NF - Privacy Reqmts (PR)” spreadsheet.

4.8 Performance Requirements

Performance requirements for the PHR System are a series of quality requirements that present the amount of performance that is expected from the PHR system implementation, operations and support. The performance requirements for the PHR also define the baseline of minimum performance measurements that the PHR solution must meet. Regardless of the growth of the PHR System, performance should be consistent and transparent to the beneficiary and other users. The scope of these requirements includes not only the Collaborative (user application) side of the PHR Solution, but also considers the performance of the MN.IT @ DHS components and communication with other systems.

Refer to the appendix for the spreadsheet containing a more detailed definition of the performance requirements. They are found on the “NF - Performance Reqmts (PE)” spreadsheet.

4.9 Systems Management Requirements

In addition to the implementation and deployment considerations for the PHR System, the State wants to ensure that operation, support and maintenance of the PHR system meets the expectations defined by the State for the users (e.g., beneficiaries, Case Managers and LTSS Providers), as well as the system components that interact with the PHR system. System management requirements will also ensure the PHR system is capable of recovering from any eventuality or dysfunction within the threshold defined by the PHR System Service Level Agreements (SLAs). Operational considerations or restrictions are also included as part of these requirements.

Refer to the appendix for the spreadsheet containing a more detailed definition of the systems management requirements. They are found on the “NF – System Mgmt Reqmts (SM)” spreadsheet.

5. SYSTEM AND USER ACCEPTANCE TESTING

5.1 Testing Phases

This section defines the high-level testing phases that will be expanded during detailed test planning. This information will be used as input to the development of test plans and is meant to be high-level information to provide a framework or starting point for the development of test plans.

5.1.1 Unit Testing

Developers use documented Unit Test guidelines subsequent or in parallel with application development to assess and correct the functionality and data problems. This will be performed by MN.IT @ DHS and Collaborative developers and/or business analysts.

5.1.2 Integration Testing

Ensures technical design and security specifications are met with the focus on interfaces and the data validation between components being joined into a larger system. This will be performed by MN.IT @ DHS and Collaborative developers and/or business analysts.

5.1.3 System Testing

System Testing is performed to assess the functionality, security and interoperability of the entire PHR system (both the DHS PHR system and Collaborative PHR system). This will be performed by MN.IT @ DHS and Collaborative developers and/or business analysts.

5.1.4 Regression Testing

Regression Testing is performed whenever changes to the system are made to ensure that a change in one area of the system does not result in unintended negative consequences in another area of the system. This will be performed by MN.IT @ DHS and Collaborative developers and/or business analysts as applicable.

5.1.5 User Acceptance Testing

User Acceptance Testing is performed to verify that the total system, both software deliverables and associated non-software deliverables (documentation, forms, procedures, etc.), will function successfully together in the business environment and will fulfill user expectations as defined in the business requirements and functional specifications. User acceptance testing normally comprises the final set of tests to be performed on the system or release. This testing will include careful attention to ensure that accessibility requirements have been fulfilled. This will be performed by MN.IT @ DHS and Collaborative users of the system components.

5.1.6 Usability Testing

Performed after the PHR has gone to production, Usability Testing will be conducted to determine what can be done to improve the user experience. This will be performed by the Collaborative with beneficiaries/legal representatives and other users.

5.2 Test Sign-off Responsibility

The IT Project Manager for MN.IT@DHS and the Project Manager for the Collaborative will be responsible for verifying that testing has been completed and that all components are ready for the next phase of testing or implementation. The PHR for LTSS Demo Project Manager will be responsible for final sign-off for all testing phases.

5.3 Major Business Processes/Scenarios

5.3.1 Beneficiary PHR Access and Use

Testing will ensure that beneficiaries/legal representatives and other beneficiary designated users can access and use the PHR as required in this Business Requirements Document and appendices, as well as subsequent design documentation that will be produced during the course of the project.

5.3.2 Case Manager and LTSS Provider PHR Access and Use

Testing will ensure that Case Managers and appropriate LTSS Providers can access and use the PHR as required in this Business Requirements Document and appendices, as well as subsequent design documentation that will be produced during the course of the project.

5.3.3 PHR Management, Operations, and Administration

Testing will ensure that Administrator users can access and use the PHR as required in this Business Requirements Document and appendices, as well as subsequent design documentation that will be produced during the course of the project.

5.3.4 Data Aggregation, Management and Display

Testing will ensure that data are securely and accurately aggregated, transmitted and displayed in the PHR as required in this Business Requirements Document and appendices, as well as subsequent design documentation that will be produced during the course of the project.

5.4 Expectations of Data Provided for Testing

5.4.1 Test Data

Unless otherwise indicated, testing will be performed using actual beneficiary data aggregated by MN.IT@DHS tools and passed securely to the Community PHR data store.

5.4.2 Time for Testing

Testing timelines will be developed as part of the test plans that are developed for each testing phase.

5.4.3 Pass/Fail Scores and Criteria

Pass/Fail scores and criteria will be included in individual test plans.

6. OPERATIONAL IMPLEMENTATION CONSIDERATIONS

6.1 Operational Impacts

Because this project is a “demonstration,” existing business processes will continue before, during and after the project’s completion.

No changes will be made to the way data are entered, stored or processed in DHS source systems as a result of this project. However, a new data aggregation tool will be created, along with customizations to an integration layer and external integration hub. These functions will enable MN.IT @ DHS to aggregate, characterize and securely publish beneficiary data to external systems in a manner not currently available within the State system.

Beneficiaries/legal representatives currently receive some information about their services and eligibility via US mail, and this will continue during the course of the project. The project will provide a secure electronic mechanism for beneficiaries/legal representatives and case managers to view information about LTSS services funded by MA.

If the demonstration successfully proves the value of a PHR for LTSS Waiver beneficiaries and it is determined by State leadership that the PHR will continue to be offered beyond the demonstration phase, “as is” business processes may be changed at that point. If State leadership decides to continue the use of the data aggregator and/or the PHR, decisions about ongoing funding for infrastructure, staffing and operations will be made at a later time.

6.2 Documentation Plan

All materials listed below must meet or exceed accessibility guidelines in the State of Minnesota’s [Accessibility Standard](#), and must follow [Plain Language Guidelines](#) as described by the Plain Language Action and Information Plan (PLAIN). Final approval of all documentation must be received from the PHR for LTSS Demo Project Manager.

Document	Description	Medium	Accountability
Data Aggregator Admin Manual	Written documentation for Data Aggregator, including descriptions and locations of all system components and source systems, and detailed instructions for administration of all functions including (but not limited to) data characterization, filtering and secure transmission, etc.	Document (available in DHS SharePoint)	MN.IT @ DHS
Collaborative PHR Admin Manual	Written documentation for Collaborative PHR administrators, including descriptions and locations of all system components and detailed instructions for administration of all functions, including (but not limited to)	Document (available online)	Collaborative

Document	Description	Medium	Accountability
	<p>PHR user authentication and access management, data verification, problem reporting, etc. An admin manual may already exist – if so, it must be enhanced to ensure that capabilities added through the PHR for LTSS Demo are well documented.</p>		
<p>Collaborative PHR User Manual</p>	<p>Written documentation for Collaborative PHR users for all user functions (beneficiaries/legal representatives, beneficiary authorized users and Case Managers), including (but not limited to):</p> <ul style="list-style-type: none"> • User Registration, • User authentication/sign-on, • Accessing information about the beneficiary’s case manager, • Accessing other information from MN DHS systems in the PHR, • Sharing access to the PHR with others at the discretion of the beneficiary/legal representative, • Entering data about the beneficiary in appropriate fields, • Getting help/accessing user support options, and • Other functions available to the user. <p>A user manual may already exist – if so, it must be enhanced to ensure that capabilities added through the PHR for LTSS Demo are well documented.</p>	<p>Document (available online)</p>	<p>Collaborative</p>
<p>Collaborative PHR User Videos</p>	<p>User videos demonstrating the use of Collaborative PHR features such as those described above.</p>	<p>Video (available online)</p>	<p>Collaborative</p>
<p>Privacy and Consent Policies</p>	<p>Written processes and policies that ensure privacy and consent safeguards that comply with HIPAA, MN Health Records Act, and MN Government Data Practices Act regulations, and that fulfill the requirements of section 12.2 of the DHS sample contract are in place for the PHR.</p>	<p>Document</p>	<p>Collaborative</p>
<p>PHR Lessons</p>	<p>Produced at the end of the</p>	<p>Document</p>	<p>PHR for LTSS</p>

Document	Description	Medium	Accountability
Learned Documentation	demonstration in a format to be determined by the State and Collaborative, which includes project successes, failures and actions that could be taken to mitigate challenges encountered by the PHR Community Collaborative in future efforts of the State to provide PHRs or beneficiary portals to service recipients.		Demo DHS Project Staff, MN.IT @ DHS, Collaborative
Testing Artifacts for e-LTSS Standard	Artifacts required by the ONC S&I Framework (which have not yet been defined) used for testing two iterations of the e-LTSS Standard as indicated in section II.B.1.m. of the RFP. The Collaborative and State will work with the ONC S&I Framework to clearly define the characteristics of this deliverable as the project progresses.	Document	PHR for LTSS Demo DHS Project Staff, Collaborative

6.3 Training Impact

Trainee	Trainer	Description
Beneficiaries/Legal Representatives and Beneficiary Authorized Users	Collaborative	Written training materials complementing the user manual and videos described above to provide in-person training on how to use the Collaborative PHR.
Case Managers and LTSS Providers	Collaborative	Written training materials complementing the user manual and videos described above to provide in-person training on how to use the Collaborative PHR.

7. DEPLOYMENT CONSIDERATIONS

Deployment strategies will be developed as the project progresses. They will require close collaboration between PHR for LTSS Demo project staff, MN.IT @ DHS staff, and Collaborative staff/vendors. Typically, tools will be deployed during regular business hours unless otherwise mutually decided by the project partners.

8. PROJECT CHANGE MANAGEMENT

Change Management is an important part of any project. Changes must be vetted and managed to ensure that they are within the scope of the project and are communicated to all stakeholders if they are approved. The process for submitting, reviewing, and approving changes must also be communicated to all stakeholders in order to properly set expectations. If changes are allowed to be submitted or are implemented in an unorganized way, any project is sure to fail. All projects must include a Change Management Plan as part of the overall Project Plan.

The Change Management approach consists of three areas:

- Ensure changes are within scope and beneficial to the project.
- Determine how the change will be implemented.
- Manage the change as it is implemented.

There are several types of changes which may be requested and considered for the PHR for LTSS Demonstration Project. Depending on the extent and type of proposed changes, changes to project documentation and the communication of these changes will be required to include any approved changes into the project plan and ensure all stakeholders are notified.

Types of changes include:

- **Scheduling Changes:** changes which will impact the approved project schedule. These changes may require fast tracking, crashing, or re-baselining the schedule depending on the significance of the impact.
- **Budget Changes:** changes which will impact the approved project budget. These changes may require requesting additional funding, releasing funding which would no longer be required, or adding to project or management reserves.
- **Scope Changes:** changes which are necessary and impact the project's scope which may be the result of unforeseen requirements which were not initially planned for. These changes may also impact budget and schedule. These changes may require revision to WBS, project scope statement, and other project documentation as necessary.

The Change Management Process that will be used for the PHR for LTSS Demo will be documented more completely in a separate document. In general terms, the process will include:

1. Change requests, which will be submitted to the PHR for LTSS Demo Project Manager by project stakeholders using a standardized change request form.
2. A Change Request register, to be maintained by the PHR for LTSS Demo Project Manager.
3. A Change Request evaluation and approval process, to be conducted by a Change Control board.

9. REFERENCES

- PHR Community Collaborative Request for Proposals
- PHR for LTSS Demo Project Charter
- PHR for LTSS Demo Project Work Plan
- PHR for LTSS Demo Project Timeline and Wave Overview

10. PHR for LTSS Demo – Glossary and Selected Acronyms

ACA - Patient Protection and Affordable Care Act (or Affordable Care Act): The Affordable Care Act actually refers to two separate pieces of legislation — the Patient Protection and Affordable Care Act (P.L. 111-148) and the Health Care and Education Reconciliation Act of 2010 (P.L. 111-152) — that, together expand Medicaid coverage to millions of low-income Americans and makes numerous improvements to both Medicaid and the Children's Health Insurance Program (CHIP).

ACH – Accountable Communities for Health: Funded by a Minnesota State Innovation Model (SIM) grant, Accountable Communities for Health work to address health problems within communities by coordinating support systems to keep people healthy. The population can include the people in a county or other geographic area, a patient population, smaller segments of a community, or other arrangements.

ACO - Accountable Care Organization: A group of health care providers with collective responsibility for patient care that helps providers coordinate services—delivering high-quality care while holding down costs.

Authorized Representative - A person authorized to act on a beneficiary's behalf as an applicant or enrollee in any of the MN health care programs. In most cases, authorized representatives have the same responsibilities and rights as applicants or enrollees. An authorized representative will receive forms, notices, and premium notices on behalf of the beneficiary. An authorized representative must be at least 18 years old and know the beneficiary's circumstances in order to provide necessary information.

Beneficiary – A consumer who receives services paid for by one of the following Medical Assistance waivers in Minnesota: Elderly Waiver (EW), Developmental Disability Waiver (DD), Community Alternatives for Disabled Individuals Waiver (CADI), Community Alternative Care Waiver (CAC), and Brain Injury (BI) Waiver. While it is possible for a person to be a recipient of non-waiver MA services, for the purposes of this RFP, the term beneficiary refers ONLY to a person who receives services paid for by an MA waiver.

BI - Brain Injury (waiver): This Minnesota MA waiver provides funding for home and community-based services for children and adults who have an acquired or traumatic brain injury and would otherwise require the level of care provided in either a nursing facility or neurobehavioral hospital. Additional details about the BI Waiver may be found on the [MN DHS web site](#).

CAC: Community Alternative Care (waiver): This Minnesota MA waiver provides funding for home and community-based services for children and adults who are chronically ill. The CAC Waiver is designed to serve people with disabilities who would otherwise require the level of care provided in a hospital. Additional details about the CAC Waiver may be found on this [MN DHS web page](#).

CADI: Community Alternatives for Disabled Individuals (waiver): This Minnesota MA waiver provides funding for home and community-based services for children and adults, who would otherwise require the level of care provided in a nursing facility. Additional details about the CADI Waiver may be found on this [MN DHS web page](#).

CB-LTSS – Community-Based Long Term Services and Supports: Refers to long-term services and supports that are delivered in homes or other community-based settings, not in institutional settings. Home and community-based services are a subset of [long-term services and supports](#).

Certified EHR – Certified Electronic Health Record: an electronic health record that is certified pursuant to section 3001(c)(5) of the HITECH Act to meet the standards and implementation specifications adopted under section 3004 as applicable.

CCD - Continuity of Care Document: The Continuity of Care Document (CCD) is a harmonized format for the exchange of clinical information, including patient demographics, medications and allergies, between patients and providers. HL7 and ASTM International created the Continuity of Care Document (CCD) to integrate two complementary healthcare data specifications: ASTM Continuity of Care Record (CCR) and HL7 Clinical Document Architecture (CDA). It uses "Web 2.0" approaches, is XML based, machine and human readable, and uses controlled vocabularies enabling computer-based decision support.

CDR – Clinical Data Repository: The CDR is the component in the Collaborative PHR that stores and manages all data collected from the source systems, including DHS source systems and clinical (EHR) source systems.

CMS - Center for Medicare and Medicaid Services: An agency within the US Department of Health & Human Services responsible for administration of several key federal health care programs. In addition to Medicare (the federal health insurance program for seniors) and Medicaid (the federal needs-based program), CMS oversees the Children's Health Insurance Program (CHIP), the Health Insurance Portability and Accountability Act ([HIPAA](#)) and the Clinical Laboratory Improvement Amendments (CLIA), among other services. Additional information about CMS can be found on their [web site](#).

DD - Developmental Disabilities (waiver): This Minnesota MA waiver provides funding for home and community-based services for children and adults with developmental disabilities or related conditions. Additional details about the DD Waiver may be found on this [MN DHS web page](#).

Degradation - The deterioration in quality, level, or standard of performance of a functional unit; a condition in which one or more of the required performance parameters fall outside predetermined limits, resulting in a lower performance. For the purposes of this project, degradation shall include the condition of one or more but not all systems, sub-systems, or data sources failing to connect. Degradation shall include speed of the user interface and availability of data sources.

DHS - Department of Human Services (Minnesota): An agency of the state of Minnesota which, working with many others, helps people meet their basic needs so they can live in dignity and achieve their highest potential. Additional information about MN DHS can be found on the [MN DHS web site](#).

EDI - Electronic Data Interchange: EDI is a direct exchange of data between two computers via the Internet or other network, using shared data formats and standards.

E-Health: The adoption and effective use of electronic health record (EHR) systems and other health information technology (HIT) including health information exchange to improve health care quality, increase patient safety, reduce health care costs, and enable individuals and communities to make the best possible health decisions.

EHR - Electronic Health Record: A real-time patient health record with access to evidence-based decision support tools that can be used to aid clinicians in decision-making. The EHR can automate and streamline a clinician's workflow, ensuring that all clinical information is communicated. It can also prevent delays in response that result in gaps in care. The EHR can also support the collection of data for uses other than clinical care, such as billing, quality management, outcome reporting, and public health disease surveillance and reporting. EHR is considered more comprehensive than the concept of an Electronic Medical Record (EMR).

EW - Elderly Waiver: This Minnesota MA waiver provides home and community-based services for people who need the level of care provided in a nursing home but who choose to live in the community. You must qualify for Medical Assistance to be eligible for Elderly Waiver services. Additional details about the Elderly Waiver may be found on this [MN DHS web page](#).

HCH – Health Care Home: A "health care home," also called a "medical home," is an approach to primary care in which primary care providers, families and patients work in partnership to improve health outcomes and quality of life for individuals with chronic health conditions and disabilities.

HDI – Health Data Intermediary: An entity that provides the infrastructure to connect computer systems or other electronic devices used by health care providers, laboratories, pharmacies, health plans, third-party administrators, or pharmacy benefit managers to facilitate the secure transmission of health information, including pharmaceutical electronic data intermediaries as defined in Minn. Stat. §62J.495, and Health Internet Service Providers (HISP) as defined by the Nationwide Health Information Network (NwHIN) Direct Project. Please note, to the extent that information is shared without the use of an intermediary, it is outside the scope of Minnesota's oversight law.

HIE - Health Information Exchange: Health information exchange or HIE means the electronic transmission of health related information between organizations according to nationally recognized standards. See the federal [Health IT web site](#) for additional information.

HIESP - Health Information Exchange Service Provider: An organization that manages security and transport for health information exchange among health care entities or

individuals. In Minnesota, certification of HIESPs is provided by MDH. See the MDH web page for more information and to see a list of State-certified HIESPs. HIESPs in Minnesota are characterized as either [Health Data Intermediaries \(HDI's\)](#) or [Health Information Organizations \(HIO's\)](#).

HIO – Health Information Organization: An entity that provides all electronic capabilities for the transmission of clinical transactions necessary for “meaningful use” of electronic health records in accordance with nationally recognized standards.

HIPAA – Health Insurance Portability and Accountability Act of 1996: There are two sections to the Act. HIPAA Title I deals with protecting health insurance coverage for people who lose or change jobs. HIPAA Title II includes an administrative simplification section which deals with the standardization of healthcare-related information systems. In the information technology industries, this section is what most people mean when they refer to HIPAA. HIPAA establishes mandatory regulations that require extensive changes to the way that health providers conduct business.

HIT (or Health IT) - Health Information Technology: The application of information processing involving both computer hardware and software that deals with the storage, retrieval, sharing, and use of health care information, data, and knowledge for communication and decision making.

HITECH Act: The Health Information Technology for Economic and Clinical Health Act in division A, title XIII, and division B, title IV, of the American Recovery and Reinvestment Act of 2009, including federal regulations adopted under that act. [Minn. Stat. §62J.495 sub. 1a(d)].

IHP - Integrated Health Partnership: This Minnesota demonstration, formerly called the Health Care Delivery Systems (HCDS) demonstration, strives to deliver higher quality and lower costs through innovative approaches to care and payment. Additional details about the IHP may be found on this [MN DHS web page](#).

Legal Representative: An attorney-in-fact (a competent adult 18 years or older who does not have to be a lawyer) under a valid power of attorney executed by the beneficiary, or a conservator or guardian appointed for the beneficiary, or a representative payee appointed for the beneficiary, or other agent of limited powers.

LTPAC - Long-term and post-acute care: Long Term and Post-Acute Care is characterized by a variety of settings, from complex care in long-term acute-care hospitals to supportive services in the community or home-based care. Typical services include rehabilitation, medical management, skilled nursing services, and assistance with activities of daily living due physical and/or cognitive impairments. Common types of LTPAC providers include but are not limited to: nursing facilities or skilled nursing facilities, home health agencies, hospice providers, inpatient rehabilitation facilities (IRFS), long-term acute care hospitals, assisted living facilities, continuing care retirement communities, home and community-based services, and adult day service providers.

LTSS – Long-term Services and Supports: On-going supports that an individual needs due to a chronic health condition or disability. These services can be delivered in a person’s home, in another community setting, or in an institutional setting. Currently, long-term services and supports is the nationally recognized term for this range of services and is used by the federal government.

MA - Medical Assistance: Medical Assistance is a jointly funded, federal-state program that pays for health care services provided to low-income individuals. It is also called Medicaid. (House Research, Nov 2014)

MITA – Medicaid Information Technology Architecture Initiative: A national framework to support improved systems development and health care management for the Medicaid enterprise. MITA has a number of goals, including development of seamless and integrated systems that communicate effectively through interoperability and common standards. See [this page](#) on the Medicaid.gov web site for more information about MITA.

MDPA - MN Government Data Practices Act: [Chapter 13 of Minnesota State Statutes](#) regulates the collection, creation, storage, maintenance, dissemination, and access to government data in government entities. It establishes a presumption that government data are public and are accessible by the public for both inspection and copying unless there is federal law, a state statute, or a temporary classification of data that provides that certain data are not public.

ONC - Office of the National Coordinator for Health Information Technology: Coordinates nationwide efforts related to the implementation and use of electronic health information exchange. ONC is organizationally located within the Office of the Secretary for the U.S. Department of Health and Human Services (HHS). Additional information about ONC can be found on the HealthIT.gov [web site](#).

Person-Centered Planning: CMS specifies that service planning for participants in Medicaid HCBS programs under section 1915(c) and 1915(i) of the Act must be developed through a person-centered planning process that addresses health and long-term services and support needs in a manner that reflects individual preferences and goals. The rules require that the person-centered planning process is directed by the individual with long-term support needs, and may include a representative whom the individual has freely chosen and others chosen by the individual to contribute to the process. See the [CMS Fact sheet on Home and Community Based Services](#) for more information.

PHR - Personal Health Record: an electronic application used by patients to maintain and manage their health information in a private, secure, and confidential environment. See [this page on the HealthIT.gov web site](#) for additional information.

PPACA - Patient Protection and Affordable Care Act: See “ACA”

Provider: For purposes of TEFT, the term “provider” is meant to include any professional who provides long-term services and supports to a MN Waiver beneficiary as part of their employment.

REACH - Regional Extension Assistance Center for Health IT: A nonprofit federal Health Information Technology Regional Extension Center dedicated to helping providers in clinics, small hospitals, and other settings in Minnesota and North Dakota implement and effectively use electronic health records. Our mission is to assure that each of our clients achieve meaningful use.

Responsible party - A person who has access to the beneficiary's income and assets and who agrees to apply the beneficiary's income and assets to pay for the beneficiary's care or who agrees to make and complete an application for medical assistance on behalf of the beneficiary.

S&I Framework – Standards & Interoperability Framework: An approach adopted by [ONC's](#) Office of Standards & Interoperability to fulfill its charge of enabling harmonized interoperability specifications to support national health outcomes and healthcare priorities, including Meaningful Use and the ongoing efforts to create better care, better population health and cost reduction through delivery improvements. More information about the S&I Framework can be found on their [web site](#).

SIM – State Innovation Model Initiative (in MN, Accountable Communities for Health): The State Innovation Models Initiative tests the ability of state governments to accelerate health transformation using the full range of regulatory and policy levers available to improve health, improve care and lower costs for the state’s citizens, including Medicare, Medicaid and Children’s Health Insurance Program beneficiaries. The State Innovation Models Initiative encourages states to develop sustainable models of multi-payer payment and delivery reform.

TEFT - Testing Experience and Functional Tools: This CMS grant program, known as TEFT (Demonstration Grant for Testing Experience and Functional Assessment Tools in Community-Based Long Term Services and Supports) is designed to test quality measurement tools and demonstrate e-health in Medicaid long term services and supports.

For definitions of additional terms related to Health IT, see the ONC’s [Glossary of Terms](#) and [Glossary of Government Acronyms](#) as well as the MN Department of Health’s [Glossary of Terms and Acronyms Related to e-Health](#).

APPENDIX – Detailed Business Requirements Workbook

Requirements defined in section 4 of the Business Requirements Document are further elaborated in the MS Excel workbook titled “Detailed Business Requirements and Budget Forms,” which can be downloaded from the [PHR for LTSS Demo web page](#).

The workbook contains multiple tabs for different types of requirements. Refer to the “Table of Contents” spreadsheet for the list and explanation of the other spreadsheets in the workbook. Refer to the Ref. Guide spreadsheet for a description of the columns included on each requirement spreadsheet.

The workbook is intended to enable Collaboratives to provide their responses as instructed in the RFP for Additional PHR Community Collaboratives to Demonstrate Personal Health Records for Beneficiaries of Long Term Services and Supports to each requirement and to enable objective evaluation of responses.

Appendix B: Detailed Business Requirements Workbook

Requirements defined in section 4 of the Business Requirements Document are further elaborated in the MS Excel workbook titled “Detailed Business Requirements and Budget Forms,” which can be downloaded from the [PHR for LTSS Demo web page](#).

The workbook contains multiple tabs for different types of requirements. Refer to the “Table of Contents” spreadsheet for the list and explanation of the other spreadsheets in the workbook. Refer to the Ref. Guide spreadsheet for a description of the columns included on each requirement spreadsheet.

The workbook is intended to enable Collaboratives to provide their responses to each requirement and to enable objective evaluation of responses.

On each requirements spreadsheet, find the row(s) where “Collaborative” or “Both” is indicated in the “Accountability – Collaborative or MN.IT @ DHS” column. These columns are NOT shaded. In those rows, fill in the “Collaborative Responses” section by entering the following information:

- **How Met:** Explain how the requirement will be met by the Collaborative PHR, or if the requirement cannot be met, indicate why. Indicate whether the required functionality already exists in the PHR, or if it would have to be added through the grant.
- **Level of Effort:** Indicate the level of effort that will be required for the Collaborative to deliver the requirement in its PHR.
- **Collaborative Solution Component Name:** Indicate the name of the specific element in the Collaborative PHR solution (application, module, plugin, etc.) where the requirement is addressed.
- **Notes:** Provide additional relevant information if needed.

The State has indicated in the “Priority” column for each requirement if it is “Critical,” “Important,” or “Useful.” See the description of the “Priority” field in the PHR Business Requirements Reference Guide at the beginning of the Detailed Requirements Workbook for definitions of these three values. Be sure that for every item that is marked “Critical,” you indicate how you will meet that requirement, or suggest an alternative that will accomplish the intent set forth by the requirement.

Appendix C: PHR for LTSS Demo – Glossary and Selected Acronyms

ACA - Patient Protection and Affordable Care Act (or Affordable Care Act): The Affordable Care Act actually refers to two separate pieces of legislation — the Patient Protection and Affordable Care Act (P.L. 111-148) and the Health Care and Education Reconciliation Act of 2010 (P.L. 111-152) — that, together expand Medicaid coverage to millions of low-income Americans and makes numerous improvements to both Medicaid and the Children's Health Insurance Program (CHIP).

ACH – Accountable Communities for Health: Funded by a Minnesota State Innovation Model (SIM) grant, Accountable Communities for Health work to address health problems within communities by coordinating support systems to keep people healthy. The population can include the people in a county or other geographic area, a patient population, smaller segments of a community, or other arrangements.

ACO - Accountable Care Organization: A group of health care providers with collective responsibility for patient care that helps providers coordinate services—delivering high-quality care while holding down costs.

Authorized Representative - A person authorized to act on a beneficiary's behalf as an applicant or enrollee in any of the MN health care programs. In most cases, authorized representatives have the same responsibilities and rights as applicants or enrollees. An authorized representative will receive forms, notices, and premium notices on behalf of the beneficiary. An authorized representative must be at least 18 years old and know the beneficiary's circumstances in order to provide necessary information.

Beneficiary – A consumer who receives services paid for by one of the following Medical Assistance waivers in Minnesota: Elderly Waiver (EW), Developmental Disability Waiver (DD), Community Alternatives for Disabled Individuals Waiver (CADI), Community Alternative Care Waiver (CAC), and Brain Injury (BI) Waiver. While it is possible for a person to be a recipient of non-Waiver MA services, for the purposes of this RFP, the term beneficiary refers ONLY to a person who receives services paid for by an MA Waiver.

BI - Brain Injury (waiver): This Minnesota MA waiver provides funding for home and community-based services for children and adults who have an acquired or traumatic brain injury and would otherwise require the level of care provided in either a nursing facility or neurobehavioral hospital. Additional details about the BI Waiver may be found on the [MN DHS web site](#).

CAC: Community Alternative Care (waiver): This Minnesota MA waiver provides funding for home and community-based services for children and adults who are chronically ill. The CAC Waiver is designed to serve people with disabilities who would otherwise require the level of care provided in a hospital. Additional details about the CAC Waiver may be found on this [MN DHS web page](#).

CADI: Community Alternatives for Disabled Individuals (waiver): This Minnesota MA waiver provides funding for home and community-based services for children and adults, who would otherwise require the level of care provided in a nursing facility. Additional details about the CADI Waiver may be found on this [MN DHS web page](#).

CB-LTSS – Community-Based Long Term Services and Supports: Refers to long-term services and supports that are delivered in homes or other community-based settings, not in institutional settings. Home and community-based services are a subset of [long-term services and supports](#).

Certified EHR – Certified Electronic Health Record: an electronic health record that is certified pursuant to section 3001(c)(5) of the HITECH Act to meet the standards and implementation specifications adopted under section 3004 as applicable.

CCD - Continuity of Care Document: The Continuity of Care Document (CCD) is a harmonized format for the exchange of clinical information, including patient demographics, medications and allergies, between patients and providers. HL7 and ASTM International created the Continuity of Care Document (CCD) to integrate two complementary healthcare data specifications: ASTM Continuity of Care Record (CCR) and HL7 Clinical Document Architecture (CDA). It uses "Web 2.0" approaches, is XML based, machine and human readable, and uses controlled vocabularies enabling computer-based decision support.

CDR – Clinical Data Repository: The CDR is the component in the Collaborative PHR that stores and manages all data collected from the source systems, including DHS source systems and clinical (EHR) source systems.

CMS - Center for Medicare and Medicaid Services: An agency within the US Department of Health & Human Services responsible for administration of several key federal health care programs. In addition to Medicare (the federal health insurance program for seniors) and Medicaid (the federal needs-based program), CMS oversees the Children’s Health Insurance Program (CHIP), the Health Insurance Portability and Accountability Act ([HIPAA](#)) and the Clinical Laboratory Improvement Amendments (CLIA), among other services. Additional information about CMS can be found on their [web site](#).

DD - Developmental Disabilities (waiver): This Minnesota MA waiver provides funding for home and community-based services for children and adults with developmental disabilities or related conditions. Additional details about the DD Waiver may be found on this [MN DHS web page](#).

Degradation - The deterioration in quality, level, or standard of performance of a functional unit; a condition in which one or more of the required performance parameters fall outside predetermined limits, resulting in a lower performance. For the purposes of this project, degradation shall include the condition of one or more but not all systems, sub-systems, or data

sources failing to connect. Degradation shall include speed of the user interface and availability of data sources.

DHS - Department of Human Services (Minnesota): An agency of the state of Minnesota which, working with many others, helps people meet their basic needs so they can live in dignity and achieve their highest potential. Additional information about MN DHS can be found on the [MN DHS web site](#).

EDI - Electronic Data Interchange: EDI is a direct exchange of data between two computers via the Internet or other network, using shared data formats and standards.

E-Health: The adoption and effective use of electronic health record (EHR) systems and other health information technology (HIT) including health information exchange to improve health care quality, increase patient safety, reduce health care costs, and enable individuals and communities to make the best possible health decisions.

EHR - Electronic Health Record: A real-time patient health record with access to evidence-based decision support tools that can be used to aid clinicians in decision-making. The EHR can automate and streamline a clinician's workflow, ensuring that all clinical information is communicated. It can also prevent delays in response that result in gaps in care. The EHR can also support the collection of data for uses other than clinical care, such as billing, quality management, outcome reporting, and public health disease surveillance and reporting. EHR is considered more comprehensive than the concept of an Electronic Medical Record (EMR).

EW - Elderly Waiver: This Minnesota MA waiver provides home and community-based services for people who need the level of care provided in a nursing home but who choose to live in the community. You must qualify for Medical Assistance to be eligible for Elderly Waiver services. Additional details about the Elderly Waiver may be found on this [MN DHS web page](#).

HCH – Health Care Home: A "health care home," also called a "medical home," is an approach to primary care in which primary care providers, families and patients work in partnership to improve health outcomes and quality of life for individuals with chronic health conditions and disabilities.

HDI – Health Data Intermediary: An entity that provides the infrastructure to connect computer systems or other electronic devices used by health care providers, laboratories, pharmacies, health plans, third-party administrators, or pharmacy benefit managers to facilitate the secure transmission of health information, including pharmaceutical electronic data intermediaries as defined in Minn. Stat. §62J.495, and Health Internet Service Providers (HISP) as defined by the Nationwide Health Information Network (NwHIN) Direct Project. Please note, to the extent that information is shared without the use of an intermediary, it is outside the scope of Minnesota's oversight law.

HIE - Health Information Exchange: Health information exchange or HIE means the electronic transmission of health related information between organizations according to nationally recognized standards. See the federal [Health IT web site](#) for additional information.

HIESP - Health Information Exchange Service Provider: An organization that manages security and transport for health information exchange among health care entities or individuals. In Minnesota, certification of HIESPs is provided by MDH. See the MDH web page for more information and to see a list of State-certified HIESPs.

HIO – Health Information Organization: An entity that provides all electronic capabilities for the transmission of clinical transactions necessary for “meaningful use” of electronic health records in accordance with nationally recognized standards.

HIPAA – Health Insurance Portability and Accountability Act of 1996: There are two sections to the Act. HIPAA Title I deals with protecting health insurance coverage for people who lose or change jobs. HIPAA Title II includes an administrative simplification section which deals with the standardization of healthcare-related information systems. In the information technology industries, this section is what most people mean when they refer to HIPAA. HIPAA establishes mandatory regulations that require extensive changes to the way that health providers conduct business.

HIT (or Health IT) - Health Information Technology: The application of information processing involving both computer hardware and software that deals with the storage, retrieval, sharing, and use of health care information, data, and knowledge for communication and decision making.

HITECH Act: The Health Information Technology for Economic and Clinical Health Act in division A, title XIII and division B, title IV of the American Recovery and Reinvestment Act of 2009, including federal regulations adopted under that act. [Minn. Stat. §62J.495 sub. 1a(d)].

IHP - Integrated Health Partnership: This Minnesota demonstration, formerly called the Health Care Delivery Systems (HCDS) demonstration, strives to deliver higher quality and lower costs through innovative approaches to care and payment. Additional details about the IHP may be found on this [MN DHS web page](#).

Legal Representative: An attorney-in-fact (a competent adult 18 years or older who does not have to be a lawyer) under a valid power of attorney executed by the beneficiary, or a conservator or guardian appointed for the beneficiary, or a representative payee appointed for the beneficiary, or other agent of limited powers.

LTPAC - Long-term and post-acute care: Long Term and Post-Acute Care is characterized by a variety of settings, from complex care in long-term acute-care hospitals to supportive services in the community or home-based care. Typical services include rehabilitation, medical management, skilled nursing services, and assistance with activities of daily living due physical

and/or cognitive impairments. Common types of LTPAC providers include but are not limited to: nursing facilities or skilled nursing facilities; home health agencies; hospice providers; inpatient rehabilitation facilities (IRFS); long-term acute care hospitals; assisted living facilities; continuing care retirement communities; home and community-based services; and adult day service providers.

LTSS – Long-term Services and Supports: On-going supports that an individual needs due to a chronic health condition or disability. These services can be delivered in a person’s home, in another community setting, or in an institutional setting. Currently, long-term services and supports is the nationally recognized term for this range of services and is used by the federal government.

MA - Medical Assistance: Medical Assistance is a jointly funded, federal-state program that pays for health care services provided to low-income individuals. It is also called Medicaid. (House Research, Nov 2014)

MITA – Medicaid Information Technology Architecture Initiative: A national framework to support improved systems development and health care management for the Medicaid enterprise. MITA has a number of goals, including development of seamless and integrated systems that communicate effectively through interoperability and common standards. See [this page](#) on the Medicaid.gov web site for more information about MITA.

MDPA - MN Government Data Practices Act: [Chapter 13 of Minnesota State Statutes](#) regulates the collection, creation, storage, maintenance, dissemination, and access to government data in government entities. It establishes a presumption that government data are public and are accessible by the public for both inspection and copying unless there is federal law, a state statute, or a temporary classification of data that provides that certain data are not public.

ONC - Office of the National Coordinator for Health Information Technology: Coordinates nationwide efforts related to the implementation and use of electronic health information exchange. ONC is organizationally located within the Office of the Secretary for the U.S. Department of Health and Human Services (HHS). Additional information about ONC can be found on the HealthIT.gov [web site](#).

Person-Centered Planning: CMS specifies that service planning for participants in Medicaid HCBS programs under section 1915(c) and 1915(i) of the Act must be developed through a person-centered planning process that addresses health and long-term services and support needs in a manner that reflects individual preferences and goals. The rules require that the person-centered planning process is directed by the individual with long-term support needs, and may include a representative whom the individual has freely chosen and others chosen by the individual to contribute to the process. See the [CMS Fact sheet on Home and Community Based Services](#) for more information.

PHR - Personal Health Record: an electronic application used by patients to maintain and manage their health information in a private, secure, and confidential environment. See [this page on the HealthIT.gov web site](#) for additional information.

PPACA - Patient Protection and Affordable Care Act: See “ACA”

Provider: For purposes of TEFT, the term “provider” is meant to include any professional who provides long-term services and supports to a MN Waiver beneficiary as part of their employment.

REACH - Regional Extension Assistance Center for Health IT: A nonprofit federal Health Information Technology Regional Extension Center dedicated to helping providers in clinics, small hospitals, and other settings in Minnesota and North Dakota implement and effectively use electronic health records. Our mission is to assure that each of our clients achieve meaningful use.

Responsible party - A person who has access to the beneficiary's income and assets and who agrees to apply the beneficiary's income and assets to pay for the beneficiary's care or who agrees to make and complete an application for medical assistance on behalf of the beneficiary.

S&I Framework – Standards & Interoperability Framework: An approach adopted by [ONC's](#) Office of Standards & Interoperability to fulfill its charge of enabling harmonized interoperability specifications to support national health outcomes and healthcare priorities, including Meaningful Use and the ongoing efforts to create better care, better population health and cost reduction through delivery improvements. More information about the S&I Framework can be found on their [web site](#).

SIM – State Innovation Model Initiative (in MN, Accountable Communities for Health): The State Innovation Models Initiative tests the ability of state governments to accelerate health transformation using the full range of regulatory and policy levers available to improve health, improve care and lower costs for the state’s citizens, including Medicare, Medicaid and Children’s Health Insurance Program beneficiaries. The State Innovation Models Initiative encourages states to develop sustainable models of multi-payer payment and delivery reform.

TEFT - Testing Experience and Functional Tools: This CMS grant program, known as TEFT (Demonstration Grant for Testing Experience and Functional Assessment Tools in Community-Based Long Term Services and Supports) is designed to test quality measurement tools and demonstrate e-health in Medicaid long term services and supports.

For definitions of additional terms related to Health IT, see the ONC’s [Glossary of Terms](#) and [Glossary of Government Acronyms](#) as well as the MN Department of Health’s [Glossary of Selected Terms and Acronyms](#).

Appendix D: Resources

The following resources are key references to understand the Minnesota Health Information Technology (HIT) landscape and provide guidance for this grant request for proposal requirements.

1. [Federal Health IT Strategic Plan, 2015 – 2020](#)
2. [MN DHS Web page for the PHR for LTSS Demo](#)
3. [State of Minnesota Accessibility Standard](#)
4. Office of the National Coordinator's [Standards & Interoperability \(S&I\) Framework](#), including their [WIKI](#) detailing the development of an electronic Long-Term Services and Supports standard.
5. [The Direct Project](#), which enables standards-based exchange of health information.
6. [CONNECT](#), an open source software solution that supports health information exchange – both locally and at the national level. CONNECT uses Nationwide Health Information Network standards and governance to make sure that health information exchanges are compatible with other exchanges being set up throughout the country
7. Office of the National Coordinator's [Data Segmentation for Privacy Standards](#) (DS4P).
8. [Minnesota e-Health Initiative](#)
9. [Minnesota e-Health Advisory Committee](#) and [Minnesota e-Health Workgroups](#)
10. [Minnesota e-Health Assessment Reports, Factsheets and Briefs](#)
11. [EHR/HIT toolkits](#)
12. Health Information Technology and Infrastructure - [2015 Interoperable Electronic Health Record Mandate](#) and MDH's [Guidance for Understanding the Minnesota 2015 Interoperable EHR Mandate](#)
13. [Electronic Prescription Drug Program](#) and MDH's [Guidance for Understanding the 2011 e-Prescribing Mandate](#)
14. [Health Information Exchange Oversight](#) in MN Statutes
15. Health Information Exchange (HIE) Oversight: [Overview of Minnesota Law](#)
16. [SMD# 16-003](#) – Letter from CMS to State Medicaid Director RE: Availability of HITECH Administrative Matching Funds to Help Professionals and Hospitals Eligible for Medicaid EHR Incentive Payments Connect to Other Medicaid Providers
17. [Request for Information: Modular Solutions for Medicaid IT Enterprise and Pre-certification of Solutions](#)
18. ONC Beacon Program findings, including those from the Southeast Minnesota Beacon Program:
 - a. [Southeast Minnesota Beacon Program](#)
 - b. [Driving Clinical Transformation in a Practice Setting with Health Information Technology- A Learning Guide](#)
 - c. [Enabling Health Information Exchange to Support Community Goals- A Learning Guide](#)
19. [Regional Extension Center for Health IT- REACH](#). REAH works with providers to improve the quality and value of care they deliver through adopting and meaningfully using HIT, specifically EHRs.

20. [Substance Abuse Mental Health Services Administration](#)
21. [Minnesota Health Records Act](#) and MDH's [Health Records Act Fact Sheet](#)
22. [Minnesota Health Records Access Study legislative report](#)

Appendix E: Responder Commitment to Require Vendor Completion of DHS Vendor Security Questionnaire



Minnesota Department of **Human Services**

The responder will require any vendor(s) with whom it contracts for design, development, testing and/or management of the required modifications to a Personal Health Record (PHR) system made under the PHR Community Collaborative grant to complete and submit a “MN Department of Human Services Vendor Security Questionnaire” and to participate in good faith to resolve problems that may arise from the vendor security scoring process.

Responder Information

PHR Community Collaborative Name: _____

Authorized Signature: _____

Printed Name: _____

Title: _____

Date: _____ Telephone Number: _____

ADA2 (12-12)

This information is available in accessible formats for individuals with disabilities by calling 651-431-3612 or by using your preferred relay service. For other information on disability rights and protections, contact the agency's ADA coordinator.

Appendix F: DHS Vendor Security Questionnaire



Minnesota Department of Human Services

MN Department of Human Services Vendor Security Questionnaire

for <project name>

Warning: This document contains nonpublic security information that cannot be disclosed to the public and should only be accessed with management approval on a need-to-know basis by authorized staff. See Minnesota Statutes §13.37, subs 1(A) and 2.

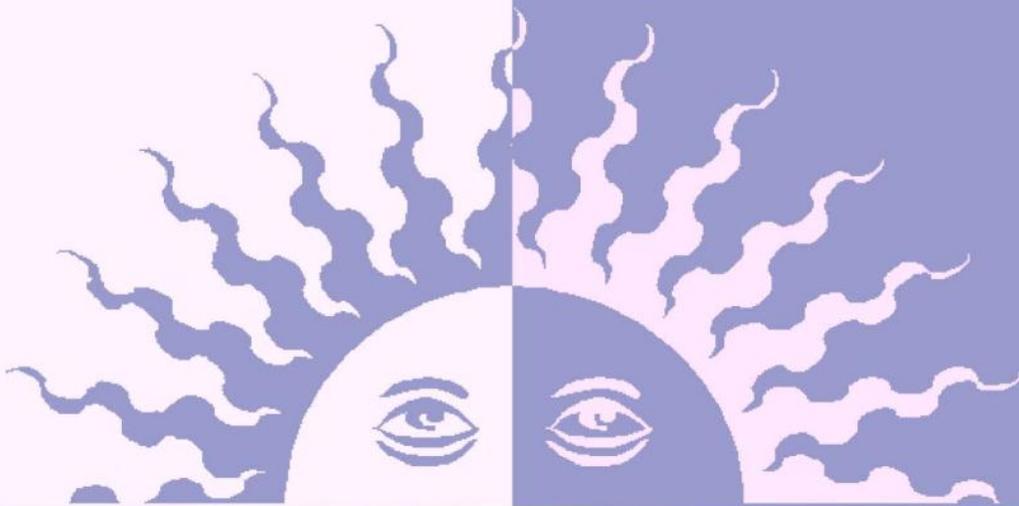


Table of Contents

Introduction and Purpose..... 3

Risk Ratings 4

Vendor Security Questionnaire..... 5

IDENTIFYING & CONTACT INFORMATION..... 5

Access to the DHS Network 6

VENDOR QUESTIONS AND SECURITY INFORMATION..... 6

Management and Policies 6

Network and Architecture..... 7

Computing Environment..... 8

Access Control..... 10

Intrusion Detection and Incident Response..... 11

Backup and Recovery..... 13

Introduction and Purpose

The purpose of this document is to obtain security information about an external vendor who may develop or host a business application for DHS, may share DHS data, or may have access to the DHS network. Security information is needed about management, policies, network architecture, computing environments, access control, intrusion detection, incident response, information backups, and disaster recovery plans to allow DHS to assess the risks that may be associated with the proposed endeavor.

The information is gathered and reviewed to ensure that vendors/Business Associates who have access to, or control of, DHS or client information, are employing effective and appropriate security standards and measures to protect that information and the DHS network. Another benefit of gathering and reviewing the information is to understand the risk associated with using a third party to provide and/or share services.

Healthcare payer and provider institutions are required by HIPAA (Health Insurance Portability and Accountability Act) to ensure the safety and confidentiality of customer information. This questionnaire is a part of the program to protect DHS and client information. The questionnaire is required for all vendors that will have control of, or access to, DHS and client information.

Upon receipt of a completed questionnaire, the responses provided will be reviewed and assigned a risk rating. The rating and any associated comments are then returned to the Business Line contact that solicited the review of the vendor. The contact in turn discusses the results with the vendor. All security concerns or recommendations must be addressed and responded to in written form prior to implementation or within a reasonable time after the risk rating has been assigned.

Responses should be sent to DHS Information Security Services at DHS.Information-Policy@state.mn.us.

This information will be kept by DHS Office of Information Security in accordance with MN State data retention policies and will not be shared outside of DHS. The information entered into this form is classified as non-public security information.

It is intended that this questionnaire be filled out, and transmitted, electronically.

Risk Ratings

Overall Risk Rating Section 1- Information Security

Check One: High
Medium
Low

Total Risk Number:
Scale: 1-55 Low; 56-110 Medium; 111-165 High

Overall Review Comments:

OIS analysis and scoring completed by:

Date:

Vendor Security Questionnaire

Note: If this vendor is providing a commercial off-the-shelf product to be used at DHS facilities, this questionnaire is not necessary. This questionnaire is for vendors that will handle, process, or store DHS or client information. Any questions should be directed to the Business Line representative with whom the vendor is working.

Identifying & Contact Information

Date of Survey:

Name of Person Completing Survey:

Vendor Name:

Name of Primary Vendor Contact:

Phone of Primary Vendor
Contact:

Name of Secondary Vendor
Contact:

Phone of Secondary Vendor
Contact:

Department in which the Vendor
Contact works:

Name of Vendor's Senior
Information Security Contact:

Phone of Vendor's Senior
Information Security Contact:

Description of the Vendor's services
to be provided:

Access to the DHS Network

Vendor Questions and Security Information

Risk Rating

Please answer the questions with enough detail to provide a thorough description of information security in your enterprise. In addition, please provide the requested documentation. ****Failure to provide the requested documentation or information may result in a higher risk rating. ****

Assigned by OIS
1=Low, 3=Medium,
5=High

Management and Policies

- 1. Has a person been assigned overall responsibility for information security? Describe the roles and responsibilities of that person. Where does this person fit into the management reporting structure?

Vendor Response:

OIS Comments:

- 2. Provide summary information on your published security policies, standards, and procedures. Are your security policies communicated to all employees, vendors and staff, and how is that accomplished?

Vendor Response:

OIS Comments:

- 3. Do you have a Policy Violation/Enforcement mechanism or procedure? Please provide a copy or a summary of this.

Vendor Response:

OIS Comments:

- 4. Do external auditors independently audit your internal audit controls? Please provide us with a copy or a summary of the results, the date of your last audit and your frequency of audit.

Vendor Response:

OIS Comments:

5. Do employees sign non-disclosure agreements regarding confidential information? If so, please attach a copy of the agreement(s) they sign, and note whether all employees sign these agreements. If some but not all employees sign agreements, state whether all employees who would have access to DHS systems/data sign agreements.

Vendor Response:

OIS Comments:

6. Do you perform criminal background and/or credit checks on your employees? If so, what is included in the check? What background/credit check feedback would prevent you hiring an applicant?

Vendor Response:

OIS Comments:

7. If applicable, do you have appropriate liability insurance/bonding/errors & omissions coverage? For each type you carry, are you willing to provide DHS a copy of the document showing the type of coverage and current policy status?

Vendor Response:

OIS Comments:

Network and Architecture

8. Provide a network architecture diagram, indicating:
- Main network components providing the service or access.
 - Any communications channels between your network and the DHS network (i.e., port numbers, protocol type).
 - Any communication channels between your network and other third-party networks which are not segregated from DHS related traffic.
 - Firewall architecture (hardware/software versions and patch process).
 - Intrusion detection products
 - Operating system platforms, databases, and applications.

Vendor Response:

OIS Comments:

9. Are the devices (routers, firewalls, and servers) handling/hosting DHS or client data dedicated to that data or do they host other entities' data as well? How is the data managed, if dedicated?

Vendor Response:

OIS Comments:

10. If the devices (routers, firewalls, and servers) are handling/hosting other entities' data, what have you done to ensure that other customers cannot access DHS data?

Vendor Response:

OIS Comments:

11. Is network traffic and the communication between application components encrypted or hashed? If yes, please describe:

- The algorithm and key length.
- Where encryption is taking place (e.g., point-to-point or only on the public network).
- What data (full message or specific fields) are encrypted? Is the data decrypted and then re-encrypted at any time?

If not, how is this communication protected?

Vendor Response:

OIS Comments:

Computing Environment

12. Where is DHS data stored? Include a description of your security measures to protect DHS data (e.g., encryption).

Vendor Response:

OIS Comments:

13. Provide summary information on your process for securing the operating system on platforms on which the application components reside. Include controls that are in place to ensure that the appropriate version of the operating system is installed with all the necessary and latest security patches and fixes.

Vendor Response:

OIS Comments:

14. Do you have separate physical/logical environments for development, testing, and production? Provide a summary description of each environment.

Vendor Response:

OIS Comments:

15. Provide summary information on your change control program(s)/process(es) governing the parts of your infrastructure which will be used to access or store DHS data or information.

Vendor Response:

OIS Comments:

16. What actions are taken when alarms are received? (For example: paging alert system for anti-virus or firewalls, network monitoring systems.) Is there 24/7 response capability?

Vendor Response:

OIS Comments:

17. Describe the operational monitoring that is in place for traffic volumes, load balancing, response times, and so on.

Vendor Response:

OIS Comments:

Access Control

18. How is access to the application handling DHS data controlled? Provide documentation on how users are identified and authenticated.

Vendor Response:

OIS Comments:

19. Provide summary information on how you will protect DHS data from vendor staff, such as employees and vendors, who don't have a "need to know." How do you assure "minimum necessary" access?

Vendor Response:

OIS Comments:

20. Provide a list and contact information (phone and email) for all persons and groups that have access to DHS Protected Information. **It is a requirement to notify DHS Office of Information Security if there is any change in this list during the project.** DHS Protected Information is defined as information, in any format, that has been identified or classified as not public, including Nonpublic Security Information, Private, Confidential, or Protected Health Information (PHI).

Vendor Response:

OIS Comments:

21. Does any component of the application or service rely on other third party service vendors?

If yes:

- Provide the vendor name.
- What process do you have in place to review their security policies and procedures?
- Has your outside provider undergone a recent (within 2 years) vulnerability assessment performed by a recognized third party? If not would they be willing to undergo a vulnerability assessment?
- Are they willing to share the assessment results with us?
- Do you have a contractual agreement with each of the parties? If so, please attach a copy of the agreements.

Vendor Response:

OIS Comments:

22. Will DHS data ever leave the physical confines of your facilities?

If yes:

- Outline the data transport method.
- Outline the data destruction method that will be used.
- Is the data encrypted before transport?
- Outline the additional controls that will be used to ensure that the data won't be disclosed or copied.

Vendor Response:

OIS Comments:

Intrusion Detection and Incident Response

23. Provide a copy or summary of the latest penetration or vulnerability assessment of your environment performed by a recognized third party. If an assessment is not available, would you arrange to have one conducted?

Vendor Response:

OIS Comments:

24. Do you conduct your own vulnerability tests? If so, provide a copy or summary of the latest results.

Vendor Response:

OIS Comments:

25. Do you receive security vulnerability advisories from organizations such as CERT? If no, explain why not. If yes, what actions are taken on these advisories? Do you have a documented process? Provide a copy or summary of your written security monitoring process to demonstrate how you remain abreast of vulnerability advisories and the actions taken to address these vulnerabilities ("patching" policies and processes).

Vendor Response:

OIS Comments:

26. Do you have an intrusion detection system deployed? If so, what type of system and brand do you use?

Vendor Response:

OIS Comments:

27. Describe the deployment of your intrusion detection system.

Vendor Response:

OIS Comments:

28. Are logs recorded, saved, and reviewed? If so, how often are the logs reviewed?

Vendor Response:

OIS Comments:

29. Provide summary information of your established computer security incident response program/plan. Include notification/escalation procedures to notify customers in the event of an incident.

Vendor Response:

OIS Comments:

Backup and Recovery

30. Provide summary information on your backup procedures. Include information on whether you do regular backups of our data or the entire data center to an off-site facility. Also include information on whether you have redundant data control centers.

Vendor Response:

OIS Comments:

31. What is the date of the most recent recovery from backup files tested to ensure integrity of the data?

Vendor Response:

OIS Comments:

32. Provide a copy or summary of your disaster recovery plan.

Vendor Response:

OIS Comments:

33. Describe your disaster recovery testing. Is it conducted periodically and are the results documented?

Vendor Response:

OIS Comments:

Appendix G: Sample State Grant Contract

State of Minnesota Department of Human Services Grant Contract

RECITALS

THIS GRANT, and amendments and supplements thereto, is between State of Minnesota, acting through its Department of Human Services _____ Division (hereinafter STATE) and _____, an independent grantee, not an employee of the State of Minnesota, address _____ (hereinafter GRANTEE), witnesseth that:

WHEREAS, the STATE, pursuant to Minnesota Statutes, section _____ is empowered to enter into contracts for the following services: _____, and

WHEREAS STATE is in need of the following services: _____, and

WHEREAS STATE is permitted to share information with the GRANTEE in accordance with Minnesota Statute, section 13.46, and

WHEREAS, GRANTEE represents that it is duly qualified and willing to perform the services set forth herein,

NOW, THEREFORE, it is agreed:

1. GRANTEE'S DUTIES. GRANTEE shall:

2. CONSIDERATION AND TERMS OF PAYMENT.

2.1 Consideration. Consideration for all services performed and goods or materials supplied by GRANTEE pursuant to this grant shall be paid by the STATE as follows:

(a.) Compensation. GRANTEE will be paid as follows

(b.) Reimbursement. Reimbursement for travel and subsistence expenses actually and necessarily incurred by GRANTEE'S performance of this grant contract shall be no greater amount than provided in the current Commissioner's Plan (which is incorporated by reference) promulgated by the Commissioner of Minnesota Management and Budget. GRANTEE shall not be reimbursed for travel and subsistence expense incurred outside the State of Minnesota unless it has received prior written approval for such out of state travel from the STATE.

(c.) Total obligation. The total obligation of the STATE for all compensation and reimbursements to GRANTEE shall not exceed _____ dollars (\$ _____).

d. (If applicable.) For compensation payable under this grant contract, which is subject to withholding under state or federal law, appropriate amounts will be deducted and withheld by the State as required.

2.2. Terms of Payment

(a.) Reimbursement shall be one initial cash advance of _____ (equal to one calendar month or calendar quarter) followed by monthly/quarterly cost reimbursement based on the previous month's/quarter's expenses as documented by receipts, invoices, travel vouchers, and time sheets.

The STATE shall issue a second cash advance of _____ (equal to one calendar month or calendar quarter) after reconciliation of the previous State fiscal year funds. If actual expenditures of the GRANTEE are less than provided in the approved program line item budget at the end of the grant's term, the STATE shall reduce the final payment so as not to exceed expenditures.

(b.) Please document the need for the Advance given to the GRANTEE:

(c.) Payments shall be made by the STATE promptly after GRANTEE'S presentation of invoices for services performed and acceptance of such services by the STATE'S authorized agent pursuant to Clause 7. Invoices shall be submitted in a form prescribed by the STATE and according to the following schedule:

(d.) (Where applicable. If blank this section does not apply.) Payments are to be made from federal funds obtained by the STATE through Title _____ of the _____ Act of _____ (Public law _____ and amendments thereto) Catalog of Federal Domestic Assistance (CFDA) No. _____ federal award name and number _____ - _____. If at any time such funds become unavailable, this grant shall be terminated immediately upon written notice of such fact by the STATE to the GRANTEE. In the event of such termination, GRANTEE shall be entitled to payment, determined on a pro rata basis, for services satisfactorily performed.

(e.) GRANTEE's Data Universal Numbering System (DUNS) number is _____. The Data Universal Numbering System (DUNS) number is the nine-digit number established and assigned by Dun and Bradstreet, Inc. (D&B) to uniquely identify business entities.

3. CONDITIONS OF PAYMENT. All services provided by GRANTEE pursuant to this grant contract shall be performed to the satisfaction of the STATE, as determined at the sole discretion of its authorized representative, and in accord with all applicable federal, state, and local laws, ordinances, rules and regulations including business registration requirements of the Office of the Secretary of State. GRANTEE shall not receive payment for work found by the STATE to be unsatisfactory, or performed in violation of federal, state or local law, ordinance, rule or regulation.

4. PAYMENT RECOUPMENT. The GRANTEE must reimburse the STATE upon demand or the STATE may deduct from future payments under this grant any amounts paid by the STATE, under this or any previous grant, for which invoices and progress reports have not been received, or for which the GRANTEE'S books, records or other documents are not sufficient to clearly substantiate that those amounts were used by the GRANTEE to perform grant services.

5. TERMS OF CONTRACT. This grant shall be effective on _____, or upon the date that the final required signature is obtained by the STATE, pursuant to Minnesota Statutes, section 16C.05, subdivision 2, whichever occurs later, and shall remain in effect through _____, or until all obligations set forth in this grant contract have been satisfactorily fulfilled, whichever occurs first. GRANTEE understands that NO work should begin under this grant contract until ALL required signatures have been obtained, and GRANTEE is notified to begin work by the STATE's Authorized Representative. The GRANTEE shall have a continuing obligation, after said grant period, to comply with the following provisions of grant clauses: 10. Indemnification; 11. State Audits; 12. Information Privacy and Security; 13. Intellectual Property Rights; 14. Publicity; and 20. Jurisdiction and Venue.

6. CANCELLATION.

6.1. For Cause or Convenience. This grant contract may be canceled by the STATE or GRANTEE at any time, with or without cause, upon thirty (30) days written notice to the other party. In the event of such a cancellation, GRANTEE shall be entitled to payment, determined on a pro rata basis, for work or services satisfactorily performed. The STATE has the right to suspend or terminate this grant contract immediately when the STATE deems the health or welfare of the service recipients is endangered, when the STATE has reasonable cause to believe that the GRANTEE has breached a material term of the grant contract, or when GRANTEE'S non-compliance with the terms of the grant contract may jeopardize federal financial participation.

6.2. Insufficient Funds. The STATE may immediately terminate this grant contract if it does not obtain funding from the Minnesota Legislature, or other funding source; or if funding cannot be continued at a level sufficient to allow for the payment of the services covered here. Termination will be by written or fax notice to the GRANTEE. The STATE is not obligated to pay for any services that are provided after notice and effective date of termination. However, the GRANTEE will be entitled to payment, determined on a pro rata basis, for services satisfactorily performed to the extent that funds are available. The STATE will not be assessed any penalty if the grant contract is terminated because of the decision of the Minnesota Legislature, or other funding source, not to appropriate funds. The STATE must provide the GRANTEE notice of the lack of funding within a reasonable time of the STATE's receiving that notice.

6.3. Breach. Notwithstanding clause 6.1., upon STATE's knowledge of a curable material breach of the grant contract by GRANTEE, STATE shall provide GRANTEE written notice of the breach and ten (10) days to cure the breach. If GRANTEE does not cure the breach within the time allowed, GRANTEE will be in default of this grant contract and STATE may cancel the grant contract immediately thereafter. If GRANTEE has breached a material term of this grant contract and cure is not possible, STATE may immediately terminate this grant contract.

7. AUTHORIZED REPRESENTATIVES, RESPONSIBLE AUTHORITY, and PROJECT MANAGER.

7.1. State. The STATE'S authorized representative for the purposes of administration of this grant contract is _____ or his/her successor. Such representative shall have final authority for

acceptance of GRANTEE'S services and if such services are accepted as satisfactory, shall so certify on each invoice submitted pursuant to Clause 2.2.

7.2. Grantee. The GRANTEE's Authorized Representative is _____ or his/her successor. If the GRANTEE's Authorized Representative changes at any time during this grant contract, the GRANTEE must immediately notify the STATE.

7.3. Information Privacy and Security. (If applicable) GRANTEE's responsible authority for the purposes of complying with data privacy and security for this grant contract is _____ or his/her successor.

7.4. Project Manager. The STATE'S project manager for this grant contract is _____ phone number: _____ or his/her successor.

8. ASSIGNMENT. GRANTEE shall neither assign nor transfer any rights or obligations under this grant contract without the prior written consent of the STATE.

9. AMENDMENTS. Any amendments to this grant contract shall be in writing, and shall be executed by the same parties who executed the original grant contract, or their successors in office.

10. INDEMNIFICATION.

In the performance of this grant contract by GRANTEE, or GRANTEE'S agents or employees, the GRANTEE must indemnify, save, and hold harmless the STATE, its agents, and employees, from any claims or causes of action, including attorney's fees incurred by the STATE, to the extent caused by GRANTEE'S: 1) Intentional, willful, or negligent acts or omissions; or 2) Actions that give rise to strict liability; or 3) Breach of contract or warranty. The indemnification obligations of this clause do not apply in the event the claim or cause of action is the result of the STATE'S sole negligence. This clause will not be construed to bar any legal remedies the GRANTEE may have for the STATE'S failure to fulfill its obligation under this grant contract.

11. STATE AUDITS. Under Minnesota Statutes, section 16C.05, subdivision 5, the books, records, documents, and accounting procedures and practices of the GRANTEE and its employees, agents, or subcontractors relevant to this grant contract shall be made available and subject to examination by the STATE, including the contracting Agency/Division, Legislative Auditor, and State Auditor for a minimum of six years from the end of this grant contract.

12. INFORMATION PRIVACY AND SECURITY.

Information privacy and security shall be governed by the "Data Sharing Agreement and Business Associate Agreement Terms and Conditions" which is attached and incorporated into this Contract as Attachment X, except that the parties further agree to comply with any agreed-upon amendments to the Data Sharing Agreement and Business Associate Agreement.

13. Intellectual Property Rights. (Option 1)

Definitions. Works means all inventions, improvements, discoveries (whether or not patentable or copyrightable), databases, computer programs, reports, notes, studies, photographs, negatives, designs, drawings, specifications, materials, tapes, and disks conceived, reduced to practice, created or originated by the GRANTEE, its employees, agents, and subcontractors, either individually or jointly with others in the performance of the grant contract. Works includes "Documents." Documents are the originals of any data bases, computer programs, reports, notes, studies, photographs, negatives, designs, drawings, specifications, materials, tapes, disks, or other materials, whether in tangible or electronic forms, prepared by the GRANTEE, its employees, agents, or subcontractors, in the performance of this grant contract.

Ownership. The STATE owns all rights, title, and interest in all of the intellectual property, including copyrights, patents, trade secrets, trademarks, and service marks in the Works and Documents created and paid for under this grant contract. The Works and Documents will be the exclusive property of the STATE and all such Works and Documents must be immediately returned to the STATE by the GRANTEE upon completion or cancellation of this grant contract. To the extent possible, those Works eligible for copyright protection under the United States Copyright Act will be deemed to be "works made for hire." If using STATE data, GRANTEE must cite the data, or make clear by referencing that STATE is the source.

Responsibilities.

Notification. Whenever any Works or Documents (whether or not patentable) are made or conceived for the first time or actually or constructively reduced to practice by the GRANTEE, including its employees and subcontractors, and are created and paid for under this grant contract, the GRANTEE will immediately give the STATE'S Authorized Representative written notice thereof, and must promptly furnish the Authorized Representative with complete information and/or disclosure thereon. The GRANTEE will assign all right, title, and interest it may have in the Works and the Documents to the STATE.

Filing and recording of ownership interests. The GRANTEE must, at the request of the STATE, execute all papers and perform all other acts necessary to transfer or record the STATE'S ownership interest in the Works and Documents created and paid for under this grant contract. The GRANTEE must perform all acts, and take all steps necessary to ensure that all intellectual property rights in these Works and Documents are the sole property of the STATE, and that neither GRANTEE nor its employees, agents, or subcontractors retain any interest in and to these Works and Documents.

Duty not to Infringe on intellectual property rights of others. The GRANTEE represents and warrants that the Works and Documents created and paid for under this grant contract do not and will not infringe upon any intellectual property rights of other persons or entities. Notwithstanding Clause 10, the GRANTEE will indemnify; defend, to the extent permitted by the Attorney General; and hold harmless the STATE, at the GRANTEE'S expense, from any action or claim brought against the STATE to the extent that it is based on a claim that all or part of these Works or Documents infringe upon the intellectual property rights of others. The GRANTEE will be responsible for payment of any and all such claims, demands, obligations, liabilities, costs, and damages, including but not limited to, attorney fees. If such a claim or action arises, or in the GRANTEE'S or the STATE'S opinion is likely to arise, the GRANTEE must, at the STATE'S discretion, either procure for the STATE the right or license to use the intellectual property rights at issue or replace or modify the allegedly infringing Works or Documents as

necessary and appropriate to obviate the infringement claim. This remedy of the STATE will be in addition to and not exclusive of other remedies provided by law.

13. Intellectual Property Rights. (Option 2)

Definitions. Works means all inventions, improvements, discoveries (whether or not patentable or copyrightable), databases, computer programs, reports, notes, studies, photographs, negatives, designs, drawings, specifications, materials, tapes, and disks conceived, reduced to practice, created or originated by the GRANTEE, its employees, agents, and subcontractors, either individually or jointly with others in the performance of this grant contract. Works includes “Documents.” Documents are the originals of any databases, computer programs, reports, notes, studies, photographs, negatives, designs, drawings, specifications, materials, tapes, disks, or other materials, whether in tangible or electronic forms, prepared by the GRANTEE, its employees, agents, or subcontractors, in the performance of this grant contract.

Use of Works and Documents. GRANTEE owns any Works or Documents developed by the GRANTEE in the performance of this grant contract. The STATE and the U.S. Department of Health and Human Services will have royalty free, non-exclusive, perpetual and irrevocable right to reproduce, publish, or otherwise use, and to authorize others to use, the Works or Documents for government purposes.

14. PUBLICITY. Any publicity given to the program, publications, or services provided resulting from this grant contract, including but not limited to, notices, informational pamphlets, press releases, research, reports, signs, and similar public notices prepared by or for the GRANTEE or its employees individually or jointly with others or any subcontractors, shall identify the STATE as the sponsoring agency and shall not be released, unless such release is a specific part of an approved work plan included in this grant contract prior to its approval by the State’s Authorized Representative.

15. HUMAN RIGHTS COMPLIANCE.

15.1 Affirmative Action requirements for Grantees with more than 40 full-time employees and a contract in excess of \$100,000. If GRANTEE has had more than 40 full-time employees within the State of Minnesota on a single working day during the previous twelve months preceding the date GRANTEE submitted its response to the STATE, it must have an affirmative action plan, approved by the Commissioner of Human Rights of the State of Minnesota, for the employment of qualified minority persons, women and persons with disabilities. See Minnesota Statutes, section 363A.36. If GRANTEE has had more than 40 full-time employees on a single working day during the previous twelve months in the state in which it has its primary place of business, then GRANTEE must either: 1) have a current Minnesota certificate of compliance issued by the Minnesota

Commissioner of Human Rights; or 2) certify that it is in compliance with federal Affirmative Action requirements.

Affirmative Action and Non-Discrimination requirements for all Grantees:

A. The GRANTEE agrees not to discriminate against any employee or applicant for employment because of race, color, creed, religion, national origin, sex, marital status, status in regard to public assistance, membership or activity in a local commission, disability, sexual orientation, or age in regard to any position for which the employee or applicant for employment is qualified. Minnesota Statutes, section 363A.02. GRANTEE agrees to take affirmative steps to employ, advance in employment, upgrade, train, and recruit minority persons, women, and persons with disabilities.

B. The GRANTEE must not discriminate against any employee or applicant for employment because of physical or mental disability in regard to any position for which the employee or applicant for employment is qualified. The GRANTEE agrees to take affirmative action to employ, advance in employment, and otherwise treat qualified disabled persons without discrimination based upon their physical or mental disability in all employment practices such as the following: employment, upgrading, demotion or transfer, recruitment, advertising, layoff or termination, rates of pay or other forms of compensation, and selection for training, including apprenticeship. Minnesota Rules, part 5000.3550

C. GRANTEE agrees to comply with the rules and relevant orders of the Minnesota Department of Human Rights issued pursuant to the Minnesota Human Rights Act.

Notification to employees and other affected parties. The GRANTEE agrees to post in conspicuous places, available to employees and applicants for employment, notices in a form to be prescribed by the commissioner of the Minnesota Department of Human Rights. Such notices will state the rights of applicants and employees, and GRANTEE’s obligation under the law to take affirmative action to employ and advance in employment qualified minority persons, women, and persons with disabilities.

The GRANTEE will notify each labor union or representative of workers with which it has a collective bargaining agreement or other contract understanding, that the GRANTEE is bound by the terms of Minnesota Statutes, section 363A.36 of the Minnesota Human Rights Act and is committed to take affirmative action to employ and advance in employment minority persons, women, and persons with physical and mental disabilities.

Compliance with Department of Human Rights Statutes. In the event of GRANTEE’s noncompliance with the provisions of this clause, actions for noncompliance may be taken in accordance with Minnesota Statutes, section 363A.36, and the rules and relevant orders issued pursuant to the Minnesota Human Rights Act.

15.2 Equal Pay Certificate.

A. Scope. Pursuant to Minnesota Statutes, section 363A.44, STATE shall not execute a contract for goods or services or an agreement for goods or services in excess of \$500,000 with a business that has 40 or more full-time employees in the State of Minnesota or a state where the business has its primary place of business on a single day during the prior 12 months, unless the business has an equal pay certificate or it has certified in writing that it is exempt.

This section does not apply to a business, with respect to a specific contract, if the commissioner of administration determines that the requirements of this Section would cause undue hardship on the business. This Section does not apply to a contract to provide goods or services to individuals under Minnesota Statutes, chapters 43A, 62A, 62C, 62D, 62E, 256B, 256I, 256L, and 268A, with a business that has a license, certification, registration, provider agreement, or provider enrollment contract that is a prerequisite to providing those good or services.

B. Consequences. If GRANTEE fails to obtain an equal pay certificate as required by Minnesota Statutes, section 363A.44 or is not in compliance with the laws identified in section 363A.44, the Minnesota Department of Human Rights (MDHR) may void this Contract on behalf of the State, and this Contract may be immediately terminated by STATE upon notice that the MDHR has suspended or revoked GRANTEE'S equal pay certificate.

C. Certification. The GRANTEE hereby certifies that it has a current equal pay certificate approved by the MDHR, that it is in compliance with the laws identified in Minnesota Statutes, section 363A.44, and is aware of the consequences for noncompliance.

16. WORKERS' COMPENSATION. The GRANTEE certifies that it is in compliance with Minnesota Statute, section 176.181, subdivision 2, pertaining to workers' compensation insurance coverage. The GRANTEE'S employees and agents will not be considered employees of the STATE. Any claims that may arise under the Minnesota Workers' Compensation Act on behalf of these employees or agents and any claims made by any third party as a consequence of any act or omission on the part of these employees or agents are in no way the STATE'S obligation or responsibility.

17. VOTER REGISTRATION REQUIREMENT. GRANTEE certifies that it will comply with Minnesota Statutes, section 201.162 by providing voter registration services for its employees and for the public served by the GRANTEE.

18. OWNERSHIP OF EQUIPMENT. Disposition of all equipment purchased under this grant contract shall be in accordance with title 45, code of federal regulations, part 92. For all equipment having a current per unit fair market value of \$5,000 or more, the STATE shall have the right to require transfer of the equipment (including title) to the Federal Government or to an eligible non-Federal party named by the STATE. This right will normally be exercised by the STATE only if the project or program for which the equipment was acquired is transferred from one grantee to another.

19. FEDERAL AUDIT REQUIREMENTS AND GRANTEE DEBARMENT INFORMATION.

GRANTEE certifies it will comply with the Single Audit Act, and Code of Federal Regulations, title 2, subtitle A, chapter II, part 200, as applicable. All sub-recipients receiving \$750,000 or more of federal assistance in a fiscal year will obtain a financial and compliance audit made in accordance with the Single Audit Act, or Code of Federal Regulations, title 2, subtitle A, chapter II, part 200, as applicable. Failure to comply with these requirements could result in forfeiture of federal funds.

DEBARMENT BY STATE, ITS DEPARTMENTS, COMMISSIONS, AGENCIES OR POLITICAL SUBDIVISIONS

GRANTEE certifies that neither it nor its principles is presently debarred or suspended by the STATE, or any of its departments, commissions, agencies, or political subdivisions. GRANTEE'S certification is a material representation upon which the grant contract award was based. GRANTEE shall provide immediate written notice to the STATE'S authorized representative if at any time it learns that this certification was erroneous when submitted or becomes erroneous by reason of changed circumstances.

CERTIFICATION REGARDING DEBARMENT, SUSPENSION, INELIGIBILITY, AND VOLUNTARY EXCLUSION

Federal money will be used or may potentially be used to pay for all or part of the work under the grant contract, therefore GRANTEE certifies that it is in compliance with federal requirements on debarment, suspension, ineligibility and voluntary exclusion specified in the solicitation document implementing Executive Order 12549. GRANTEE'S certification is a material representation upon which the grant contract award was based.

20. JURISDICTION AND VENUE. This grant contract, and amendments and supplements thereto, shall be governed by the laws of the State of Minnesota. Venue for all legal proceedings arising out of this grant contract, or breach thereof, shall be in the state or federal court with competent jurisdiction in Ramsey County, Minnesota.

21. WAIVER. If the State fails to enforce any provision of this grant contract, that failure does not waive the provision or the STATE's right to enforce it.

22. CONTRACT COMPLETE. This grant contract contains all negotiations and agreements between the STATE and the GRANTEE. No other understanding regarding this grant contract, whether written or oral may be used to bind either party.

23. OTHER PROVISIONS.

23.1. GRANTEE agrees that it will at all times during the term of the grant contract keep in force a commercial general liability insurance policy with the following minimum amounts: \$2,000,000 per occurrence and \$2,000,000 annual aggregate, protecting it from claims for damages for bodily injury, including sickness or disease, death, and for care and loss of services as well as from claims for property damage, including loss of use which may arise from operations under the grant contract whether the

operations are by the GRANTEE or by a subcontractor or by anyone directly or indirectly employed by the GRANTEE under the grant contract.

23.2. The GRANTEE further agrees to keep in force a blanket employee theft/employee dishonesty policy in at least the total amount of the first year's grant award as either an addendum on its property insurance policy, or, if it is not feasible to include it as an addendum to a property insurance policy, as a stand-alone employee theft/employee dishonesty policy. The STATE will be named as both a joint payee and a certificate holder on the employee theft/employee dishonesty addendum or on the stand-alone employee theft/employee dishonesty policy, whichever is applicable. Only in cases in which the first year's grant award exceeds the available employee theft/employee dishonesty coverage may grantees provide blanket employee theft/employee dishonesty insurance in an amount equal to either 25% of the yearly grant amount, or the first quarterly advance amount, whichever is greater. Upon execution of this grant contract, the GRANTEE shall furnish the State with a certificate of employee theft/employee dishonesty insurance.

23.3. GRANTEE agrees that no religious based counseling shall take place under the auspices of this grant contract.

23.4. If the GRANTEE has an independent audit, a copy of the audit shall be submitted to the STATE.

23.5. Payment to Subcontractors. (If applicable) As required by Minnesota Statutes, section 16A.1245, the prime GRANTEE must pay all subcontractors, less any retainage, within ten (10) calendar days of the prime GRANTEE's receipt of payment from the State for undisputed services provided by the subcontractor(s) and must pay interest at the rate of one and one-half percent per month or any part of a month to the subcontractor(s) on any undisputed amount not paid on time to the subcontractor(s).

Appendix H: Sample Data Sharing and Business Associate Agreement

STATE OF MINNESOTA DEPARTMENT OF HUMAN SERVICES DATA SHARING AND BUSINESS ASSOCIATE AGREEMENT

THIS DATA SHARING AGREEMENT, and amendments and supplements thereto (“Agreement”), are between the State of Minnesota, acting through its Department of Human Services, DIVISION, (“STATE”) and the PARTY (“DATA SHARING PARTNER”).

RECITALS

This Agreement sets forth the terms and conditions in which STATE will share data with and permit DATA SHARING PARTNER to use or disclose Protected Information that the parties are legally required to safeguard pursuant to the Minnesota Data Practices Act under Minnesota Statutes, chapter 13, the Health Insurance Portability and Accountability Act rules and regulations codified at 45 C.F.R. Parts 160, 162, and 164 (“HIPAA”) and other applicable laws.

The parties agree to comply with all applicable provisions of the Minnesota Data Practices Act, HIPAA, and any other state and federal statutes that apply to the Protected Information.

General Description of Protected Information That Will Be Shared: For example, “Minnesota Health Programs claims data for fiscal years 2013 through 2014”; and

Purpose for Sharing Protected Information and Expected Outcomes: Please describe why sharing the information is necessary to accomplish the particular purpose of a grant, contract or other program mission. For example, “Review Minnesota Health Programs to program integrity, quality, and effectiveness.”

STATE is permitted to share the Protected Information with DATA SHARING PARTNER pursuant to [Legal Authority: The statutes, regulations, rules, and/or standards that allow the Protected Information to be shared. Include, if applicable in the case of a specific program area project or a grant contract, references to state or federal legislation authorizing the grant or project]

It is expressly agreed that DATA SHARING PARTNER is a “business associate” of STATE, as defined by HIPAA under 45 C.F.R. § 160.103. The disclosure of protected health information to GRANTEE that is subject to the Health Insurance Portability Accountability Act (HIPAA) is permitted by 45 C.F.R. § 164.502(e)(1)(i).

It is understood by DATA SHARING PARTNER that, as a business associate under HIPAA, DATA SHARING PARTNER is directly liable under the HIPAA Rules and subject to civil and, in some cases, criminal penalties for making uses and disclosures of protected health information that are not authorized by contract or required by law. DATA SHARING PARTNER is also directly liable and subject to civil penalties for failing to safeguard electronic protected health information in accordance with the HIPAA Security Rule.

The parties therefore agree as follows:

DEFINITIONS

- A. "Agent" means DATA SHARING PARTNER'S employees, contractors, subcontractors, and other non-employees and representatives.
- B. "Applicable Safeguards" means the state and federal provisions listed in Section 6.1 of this agreement.
- C. "Breach" means the acquisition, access, use, or disclosure of unsecured protected health information in a manner not permitted by HIPAA, which compromises the security or privacy of protected health information.
- D. "Business associate" shall generally have the same meaning as the term "business associate" at 45 C.F.R. § 160.103, and in reference to the party to this agreement, shall mean DATA SHARING PARTNER.
- E. "Disclosure" means the release, transfer, provision of access to, or divulging in any manner of information by the entity in possession of the Protected Information.
- F. "HIPAA" means the rules and regulations codified at 45 C.F.R. Parts 160, 162, and 164.
- G. "Individual" means the person who is the subject of protected information.
- H. "Privacy incident" means a violation of an information privacy provision of any applicable state and federal law, statute, regulation, rule, or standard, including those listed in this Agreement.
- I. "Protected information" means any information that is or will be used by STATE or DATA SHARING PARTNER under this Agreement that is protected by federal or state privacy laws, statutes, regulations or standards, including those listed in this Agreement. This includes, but is not limited to, individually identifiable information about a State, county or tribal human services agency client or a client's family member. Protected information also includes, but is not limited to, protected health information, as defined below, and protected information maintained within or accessed via a State information management system, including a State "legacy system" and other State application.
- J. "Protected health information" is a subset of "individually identifiable health information" in accordance with 45 C.F.R. § 160.103, but for purposes of this Agreement refers only to that information that is received, created, maintained, or transmitted by DATA SHARING PARTNER as a business associate on behalf of DHS. Protected health information is a specific subset of protected information as defined above.
- K. "Security incident" means the attempted or successful unauthorized use or the interference with system operations in an information management system or application. Security incident does not include pings and other broadcast attacks on a system's firewall, port scans, unsuccessful log-on attempts, denials of service, and any combination of the above, provided that such activities do not result in the unauthorized use of Protected Information.

- L. "Use" or "used" means any activity by the parties during the duration of this Agreement involving protected information including its creation, collection, access, use, modification, employment, application, utilization, examination, analysis, manipulation, maintenance, dissemination, sharing, disclosure, transmission, or destruction. Use includes any of these activities whether conducted manually or by electronic or computerized means.
- M. "User" means an agent of either party, who has been authorized to use protected information.

1. Term of Contract.

- 1.1 Effective date.** The effective date of this Agreement is _____, or the date this Agreement is signed by both parties, whichever is later.
- 1.2 Expiration date.** The expiration date of this Agreement is _____ or until all obligations set forth in this Agreement have been satisfactorily fulfilled, whichever occurs first.

2. Duties.

- 2.1 STATE will disclose the following information to DATA SHARING PARTNER:
- 2.2 DATA SHARING PARTNER shall:

3. Time. The parties will perform their duties within the time limits established in this Agreement unless prior written approval is obtained from the other party.

4. Consideration and Payment. There will be no funds obligated by either party under this Agreement. Each party will be responsible for its own costs in performing its stated duties.

5. Authorized Representatives and Responsible Authority.

- 5.1 State.** STATE's authorized representative is **Name and division or title**, or his/her successor. DATA SHARING PARTNER shall make any notice or contact to STATE required by this Agreement to STATE's authorized representative.
- 5.2 Data Sharing Partner.** DATA SHARING PARTNER's Authorized Representative is **Name and title** or his/her successor.
- 5.3 Information Privacy and Security.** STATE's responsible party for the purposes of complying with the Applicable Safeguards in this Agreement is STATE's authorized representative. DATA SHARING PARTNER's responsible party for the purposes of complying with the Applicable Safeguards this Agreement is **Name and title** or his/her successor.

6. Information Privacy and Security.

DATA SHARING PARTNER and STATE must comply with the Minnesota Government Data Practices Act, Minn. Stat. § 13, and the Health Insurance Portability Accountability Act ["HIPAA"], 45 C.F.R. § 164.103, et seq., as it applies to all data provided by STATE under this

Agreement, and as it applies to all data created, collected, received, stored, used, maintained, or disseminated by DATA SHARING PARTNER under this Agreement. The civil remedies of Minn. Stat. § 13.08 apply to DATA SHARING PARTNER and STATE. Additionally, the remedies of HIPAA apply to the release of data governed by that Act.

6.1 Compliance with Applicable Safeguards.

- A. State and Federal Safeguards.** The parties acknowledge that the Protected Information to be shared under the terms of this Agreement may be subject to one of the following laws, statutes, regulations, rules, and standards, as applicable (“Applicable Safeguards”). The parties agree to comply with all rules, regulations and laws, including as amended or revised, applicable to the exchange, use and disclosure of data under this Agreement.
1. Health Insurance Portability and Accountability Act rules and regulations codified at 45 C.F.R. Parts 160, 162, and 164 (“HIPAA”);
 2. Minnesota Government Data Practices Act (Minn. Stat. Chapter 13);
 3. Minnesota Health Records Act (Minn. Stat. §144.291 - 144.298);
 4. Confidentiality of Alcohol and Drug Abuse Patient Records (42 U.S.C. § 290dd-2 and 42 C.F.R. § 2.1 to §2.67);
 5. Tax Information Security Guidelines for Federal, State and Local Agencies (26 U.S.C. 6103 and Publication 1075);
 6. U.S. Privacy Act of 1974;
 7. Computer Matching Requirements (5 U.S.C. 552a);
 8. Social Security Data Disclosure (section 1106 of the Social Security Act);
 9. Disclosure of Information to Federal, State and Local Agencies (DIFSLA Handbook” Publication 3373);
 10. Final Exchange Privacy Rule of the Affordable Care Act (45 C.F.R. § 155.260); and
 11. NIST Special Publication 800-53, Revision 4 (NIST.SP.800-53r4).
- B. Statutory Amendments and Other Changes to Applicable Safeguards.** The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary to ensure, current, ongoing compliance with the requirements of the laws listed in this Section or in any other applicable law.

6.2 DATA SHARING PARTNER Data Responsibilities

A. Use Limitation.

1. **Restrictions on Use and Disclosure of Protected Information.** Except as otherwise authorized in this Agreement, DATA SHARING PARTNER may only use or disclose Protected Information as necessary to provide the services to STATE as described herein, or as otherwise required by law, provided that such use or disclosure of Protected Information, if performed by STATE, would not violate this Agreement, HIPAA, or other state and federal statutes or regulations that apply to the Protected Information.

2. **Federal tax information.** To the extent that Protected Information used under this Agreement constitutes “federal tax information” (FTI), DATA SHARING PARTNER shall ensure that this data only be used as authorized under the Patient Protection and Affordable Care Act, the Internal Revenue Code, 26 U.S.C. § 6103(C), and IRS Publication 1075.

B. **Individual Privacy Rights.** DATA SHARING PARTNER shall ensure individuals are able to exercise their privacy rights regarding Protected Information, including but not limited to the following:

1. **Complaints.** DATA SHARING PARTNER shall work cooperatively with STATE to resolve complaints received from an individual; from an authorized representative; or from a state, federal, or other health oversight agency.

2. **Amendments to Protected Information Requested by Data Subject Generally.** Within ten (10) business days, DATA SHARING PARTNER must forward to STATE any request to make any amendment(s) to Protected Information in order for STATE to satisfy its obligations under Minn. Stat. § 13.04, subd. 4. If the request to amend Protected Information pertains to Protected Health Information, then DATA SHARING PARTNER must also make any amendment(s) to protected health information as directed or agreed to by STATE pursuant to 45 C.F.R. § 164.526 or otherwise act as necessary to satisfy STATE or DATA SHARING PARTNER’s obligations under 45 CF.R. § 164.526 (including, as applicable, protected health information in a designated record set).

C. **Background Review and Reasonable Assurances Required of Agents.**

1. **Criminal Background Check Required.** DATA SHARING PARTNER and employees of DATA SHARING PARTNER accessing STATE’s Protected Information must submit to STATE or provide evidence of a computerized criminal history system background check (hereinafter “CCH background check”) performed within the last 12 months before work can begin under this Agreement. “CCH background check” is defined as a background check including search of the computerized criminal history system of the Minnesota Department of Public Safety’s Bureau of Criminal Apprehension.

2. **Reasonable Assurances.** DATA SHARING PARTNER represents that, before its Agents are allowed to use or disclose Protected Information, DATA SHARING PARTNER has conducted and documented a background review of such Agents sufficient to provide DATA SHARING PARTNER with reasonable assurances that the Agent will comply with the terms of this Agreement and Applicable Safeguards.

3. **Documentation.** DATA SHARING PARTNER shall make available documentation required by this Section upon request by STATE.

D. Ongoing Responsibilities to Safeguard Protected Information.

1. **Privacy and Security Policies.** DATA SHARING PARTNER shall develop, maintain, and enforce policies, procedures, and administrative, technical, and physical safeguards to ensure the privacy and security of the Protected Information.
2. **Electronic Protected Information.** DATA SHARING PARTNER shall implement and maintain appropriate safeguards, and comply with Subpart C of 45 C.F.R. Part 164 (HIPAA Security Rule) with respect to electronic Protected Information, including electronic Protected Health Information, to prevent the use or disclosure other than as provided for by this Agreement.
3. **Monitoring Agents.** DATA SHARING PARTNER shall ensure that any contractor, subcontractor, or other agent to whom DATA SHARING PARTNER discloses Protected Information on behalf of STATE, or whom DATA SHARING PARTNER employs or retains to create, receive, use, store, disclose, or transmit Protected Information on behalf of STATE, agrees to the same restrictions and conditions that apply to CONTRACTOR under this Agreement with respect to such Protected Information, and in accordance with 45 C.F.R. §§ 164.502(e)(1)(ii) and 164.308(b)(2).
4. **Minimum Necessary Access to Protected Information.** DATA SHARING PARTNER shall ensure that its Agents use only the minimum necessary Protected Information needed to complete an authorized and legally permitted activity.
5. **Training.** DATA SHARING PARTNER shall ensure that Agents are properly trained and comply with all Applicable Safeguards and the terms of this Agreement.

E. Responding to Privacy Incidents, Security Incidents, and Breaches. DATA SHARING PARTNER will comply with this Section for all protected information shared under this Agreement. Additional obligations for specific kinds of protected information shared under this Agreement are addressed in Section 6.2(F).

1. **Mitigation of harmful effects.** Upon discovery of any actual or suspected privacy incident, security incident, or breach, DATA SHARING PARTNER will mitigate, to the extent practicable, any harmful effect of the privacy incident, security incident, or breach. Mitigation may include, but is not limited to, notifying and providing credit monitoring to affected individuals.

2. **Investigation.** Upon discovery of any actual or suspected privacy incident, security incident, or breach, DATA SHARING PARTNER will investigate to (1) determine the root cause of the incident, (2) identify individuals affected, (3) determine the specific protected information impacted, and (4) comply with notification and reporting provisions of this Agreement and applicable law.
3. **Corrective action.** Upon identifying the root cause of any privacy incident, security incident, or breach, DATA SHARING PARTNER will take corrective action to prevent, or reduce to the extent practicable, any possibility of recurrence. Corrective action may include, but is not limited to, patching information system security vulnerabilities, employee sanctions, or revising policies and procedures.
4. **Notification to individuals and others; costs incurred.**
 - a. **Protected Information.** DATA SHARING PARTNER will determine whether notice to data subjects and/or any other external parties regarding any privacy incident or security incident is required by law. If such notice is required, DATA SHARING PARTNER will comply with STATE's and DATA SHARING PARTNER's obligations under any applicable law requiring notification, including, but not limited to, Minn. Stat. §§ 13.05 and 13.055.
 - b. **Protected Health Information.** If a privacy incident or security incident results in a breach of protected health information, as these terms are defined in this Agreement, then DATA SHARING PARTNER will provide notice to individual data subjects under any applicable law requiring notification, including but not limited to providing notice as outlined in 45 C.F.R. § 164.404.
 - c. **Failure to notify.** If DATA SHARING PARTNER fails to notify individual data subjects or other external parties under subparagraphs (a) and (b), then DATA SHARING PARTNER will reimburse STATE for any costs STATE incurs as a result of DATA SHARING PARTNER's failure to provide notification.
5. **Obligation to report to STATE.** Upon discovery of a privacy incident, security incident, or breach, DATA SHARING PARTNER will report to STATE in writing as specified in Section 6.2(F).
 - a. **Communication with authorized representative.** DATA SHARING PARTNER will send any written reports to, and communicate and coordinate as necessary with, STATE's authorized representative.
 - b. **Cooperation of response.** DATA SHARING PARTNER will cooperate with requests and instructions received from STATE regarding

activities related to investigation, containment, mitigation, and eradication of conditions that led to, or resulted from, the security incident, privacy incident, or breach.

- c. **Information to respond to inquiries about an investigation.** DATA SHARING PARTNER will, as soon as possible, but not later than forty-eight (48) hours after a request from STATE, provide STATE with any reports or information requested by STATE related to an investigation of a security incident, privacy incident, or breach.

6. **Documentation.** DATA SHARING PARTNER will document actions taken under paragraphs 1 through 5 of this Section, and provide such documentation to STATE upon request.

- F. **Reporting Privacy Incidents, Security Incidents, and Breaches.** DATA SHARING PARTNER will comply with the reporting obligations of this Section as they apply to the kind of protected information involved. DATA SHARING PARTNER will also comply with Section 6.2(E) above in responding to any privacy incident, security incident, or breach.

1. **[OPTIONAL] Federal Tax Information.** DATA SHARING PARTNER will report all actual or suspected unauthorized uses or disclosures of federal tax information (FTI). FTI is information protected by Tax Information Security Guidelines for Federal, State and Local Agencies (26 U.S.C. § 6103 and Publication 1075).

- a. **Initial report.** DATA SHARING PARTNER will, in writing, immediately report all actual or suspected unauthorized uses or disclosures of FTI to STATE. DATA SHARING PARTNER will include in its initial report to STATE all information under Section 6.2(E)(1)-(4), of this Agreement that is available to DATA SHARING PARTNER at the time of the initial report.

- b. **Final report.** DATA SHARING PARTNER will, upon completion of its investigation of and response to any actual or suspected unauthorized uses or disclosures of FTI, or upon STATE's request in accordance with Section 6.2(E)(5) submit in writing a report to STATE documenting all actions taken under Section 6.2(E)(1)-(4), of this agreement.

2. **[OPTIONAL] Social Security Administration Data.** DATA SHARING PARTNER will report all actual or suspected unauthorized uses or disclosures of Social Security Administration (SSA) data. SSA data is information protected by section 1106 of the Social Security Act.

- a. **Initial report.** DATA SHARING PARTNER will, in writing, immediately report all actual or suspected unauthorized uses or disclosures of SSA data to STATE. DATA SHARING PARTNER will include in its initial

report to STATE all information under Section 6.2(E)(1)-(4), of this Agreement that is available to DATA SHARING PARTNER at the time of the initial report.

- b. **Final report.** DATA SHARING PARTNER will, upon completion of its investigation of and response to any actual or suspected unauthorized uses or disclosures of SSA data, or upon STATE's request in accordance with Section 6.2(E)(5) submit in writing a report to STATE documenting all actions taken under Section 6.2(E)(1)-(4), of this agreement.

3. Protected Health Information. DATA SHARING PARTNER will report breaches and security incidents involving protected health information to STATE and other external parties. DATA SHARING PARTNER will notify STATE, in writing, of (1) any breach or suspected breach of protected health information; (2) any security incident; or (3) any violation of an individual's privacy rights as they involve protected health information created, received, maintained, or transmitted by DATA SHARING PARTNER or its Agents on behalf of STATE.

- a. **Breach reporting.** DATA SHARING PARTNER will report, in writing, any breach of protected health information to STATE within five (5) business days of discovery, in accordance with 45 C.F.R § 164.410.

Content of report to STATE. Reports to the authorized representative regarding breaches of protected health information will include:

1. Identities of the individuals whose unsecured Protected Health Information has been breached.
2. Date of the breach and date of its discovery.
3. Description of the steps taken to investigate the breach, mitigate its effects, and prevent future breaches.
4. Sanctions imposed on members of DATA SHARING PARTNER's workforce involved in the breach.
5. Other available information that is required to be included in notification to the individual under 45 C.F.R. § 164.404(c).
6. Statement that DATA SHARING PARTNER has notified, or will notify, affected data subjects in accordance with 45 C.F.R. § 164.404.

- b. **Security incidents resulting in a breach.** DATA SHARING PARTNER will report, in writing, any security incident that results in a breach, or suspected breach, of protected health information to STATE within five (5) business days of discovery, in accordance with 45 C.F.R § 164.314 and 45 C.F.R § 164.410.

- c. **Security incidents that do not result in a breach.** DATA SHARING PARTNER will report all security incidents that do not result in a

breach, but involve systems maintaining protected health Information created, received, maintained, or transmitted by DATA SHARING PARTNER or its Agents on behalf of STATE, to STATE on a monthly basis, in accordance with 45 C.F.R § 164.314.

- d. **Other violations.** DATA SHARING PARTNER will report any other violation of an individual's privacy rights as it pertains to protected health information to STATE within five (5) business days of discovery. This includes, but is not limited to, violations of HIPAA data access or complaint provisions.
- e. **Reporting to other external parties.** DATA SHARING PARTNER will report all breaches of protected health information to the federal Department of Health and Human Services, as specified under 45 C.F.R 164.408. If a breach of protected health information involves 500 or more individuals:
 - 1. DATA SHARING PARTNER will immediately notify STATE.
 - 2. DATA SHARING PARTNER will report to the news media and federal Department of Health and Human Services in accordance with 45 C.F.R. §§ 164.406-408.

4. Other Protected Information. DATA SHARING PARTNER will report all other privacy incidents and security incidents to STATE.

- a. **Initial report.** DATA SHARING PARTNER will report all other privacy and security incidents to STATE, in writing, within five (5) days of discovery. If DATA SHARING PARTNER is unable to complete its investigation of, and response to, a privacy incident or security incident within five (5) days of discovery, then DATA SHARING PARTNER will provide STATE with all information under Section 6.2(E)(1)-(4), of this Agreement that are available to DATA SHARING PARTNER at the time of the initial report.
- b. **Final report.** DATA SHARING PARTNER will, upon completion of its investigation of and response to a privacy incident or security incident, or upon STATE's request in accordance with Section 6.2(E), paragraph 5, submit in writing a report to STATE documenting all actions taken under Section 6.2(E)(1)-(4), of this agreement.

G. Designated Record Set—Protected Health Information. If, on behalf of STATE, DATA SHARING PARTNER maintains a complete or partial designated record set, as defined in 45 C.F.R. § 164.501, upon request by STATE, DATA SHARING PARTNER shall:

- 1. Provide the means for an individual to access, inspect, or receive copies of the individual's Protected Health Information.

2. Provide the means for an individual to make an amendment to the individual's Protected Health Information.
3. Provide the means for access and amendment in the time and manner that complies with HIPAA or as otherwise directed by STATE.

H. Access to Books and Records, Security Audits, and Remediation. DATA SHARING PARTNER shall conduct and submit to audits and necessary remediation as required by this Section to ensure compliance with all Applicable Safeguards and the terms of this Agreement.

1. DATA SHARING PARTNER represents that it has audited and will continue to regularly audit the security of the systems and processes used to provide services under this Agreement, including, as applicable, all data centers and cloud computing or hosting services under contract with DATA SHARING PARTNER. DATA SHARING PARTNER will conduct such audits in a manner sufficient to ensure compliance with the security standards referenced in this Agreement.
2. This security audit required above will be documented in a written audit report which will, to the extent permitted by applicable law, be deemed confidential security information and not public data under the Minnesota Government Data Practices Act, Minn. Stat. § 13.37, subd. 1(a) and 2(a).
3. DATA SHARING PARTNER agrees to make its internal practices, books, and records related to its obligations under this Agreement available to STATE or a STATE designee upon STATE's request for purposes of conducting a financial or security audit, investigation, or assessment, or to determine DATA SHARING PARTNER's or STATE's compliance with Applicable Safeguards, the terms of this agreement and accounting standards. For purposes of this provision, other authorized government officials includes, but is not limited to, the Secretary of the United States Department of Health and Human Services.
4. DATA SHARING PARTNER will make and document best efforts to remediate any control deficiencies identified during the course of its own audit(s), or upon request by STATE or other authorized government official(s), in a commercially reasonable timeframe.

I. Documentation Required. Any documentation required by this Agreement, or by applicable laws, standards, or policies, of activities including the fulfillment of requirements by DATA SHARING PARTNER, or of other matters pertinent to the execution of this Agreement, must be securely maintained and retained by DATA SHARING PARTNER for a period of six years from the date of expiration or termination of this Agreement, or longer if required by applicable law, after which the documentation must be disposed of consistent with Section 6.6 of this Agreement.

DATA SHARING PARTNER shall document disclosures of Protected Health Information made by DATA SHARING PARTNER that are subject to the accounting of disclosure requirement described in 45 C.R.F. 164.528, and shall provide to STATE such documentation in a time and manner designated by STATE at the time of the request.

- J. Requests for Disclosure of Protected Information.** If DATA SHARING PARTNER or one of its Agents receives a request to disclose Protected Information, DATA SHARING PARTNER shall inform STATE of the request and coordinate the appropriate response with STATE. If DATA SHARING PARTNER discloses Protected Information after coordination of a response with STATE, it shall document the authority used to authorize the disclosure, the information disclosed, the name of the receiving party, and the date of disclosure. All such documentation shall be maintained for the term of this Agreement and shall be produced upon demand by STATE.
- K. Conflicting Provisions.** DATA SHARING PARTNER shall comply with all applicable provisions of HIPAA and with this Agreement. To extent that the parties determine, following consultation, that the terms of this Agreement are less stringent than the Applicable Safeguards, DATA SHARING PARTNER must comply with the Applicable Safeguards. In the event of any conflict in the requirements of the Applicable Safeguards, DATA SHARING PARTNER must comply with the most stringent Applicable Safeguard.
- L. Data Availability.** DATA SHARING PARTNER, or any entity with legal control of any protected information provided by STATE, shall make any and all protected information available to STATE upon request within a reasonable time as is necessary for STATE to comply with applicable law.

6.3 Data Security.

- A. STATE Information Management System Access.** If STATE grants DATA SHARING PARTNER access to Protected Information maintained in a STATE information management system (including a STATE “legacy” system) or in any other STATE application, computer, or storage device of any kind, then DATA SHARING PARTNER agrees to comply with any additional system- or application-specific requirements as directed by STATE.
- B. Electronic Transmission.** The parties agree to encrypt electronically transmitted Protected Information in a manner that complies with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; 800-113, Guide to SSL VPNs, or others methods validated under Federal Information Processing Standards (FIPS) 140-2.
- C. Portable Media and Devices.** The parties agree to encrypt Protected Information written to or stored on portable electronic media or computing

devices in a manner that complies with NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices.

6.4 DATA SHARING PARTNER Permitted Uses and Responsibilities.

- A. Management and Administration.** Except as otherwise limited in this Agreement, DATA SHARING PARTNER may:
1. Use Protected Health Information for the proper management and administration of DATA SHARING PARTNER or to carry out the legal responsibilities of DATA SHARING PARTNER.
 2. Disclose Protected Health Information for the proper management and administration of DATA SHARING PARTNER, provided that:
 - a. The disclosure is required by law; or
 - b. The disclosure is required to perform the services provided to or on behalf of STATE or the disclosure is otherwise authorized by STATE, and DATA SHARING PARTNER:
 - i. Obtains reasonable assurances, in the form of a data sharing agreement, from the entity to whom the Protected Health Information will be disclosed that the Protected Health Information will remain confidential, and will not be used or disclosed other than for the contracted services or the authorized purposes; and
 - ii. DATA SHARING PARTNER requires the entity to whom Protected Health Information is disclosed to notify DATA SHARING PARTNER of any compromise to the confidentiality of Protected Health Information of which it becomes aware.
- B. Notice of Privacy Practices.** If DATA SHARING PARTNER's duties and responsibilities require it, on behalf of STATE, to obtain individually identifiable health information from individual(s), then DATA SHARING PARTNER shall, before obtaining the information, confer with STATE to ensure that any required Notice of Privacy Practices includes the appropriate terms and provisions.
- C. De-identify Protected Health Information.** DATA SHARING PARTNER may use Protected Health Information to create de-identified Protected Health Information provided that DATA SHARING PARTNER complies with the de-identification methods specified in 45 C.F.R. § 164.514.
- D. Aggregate Protected Health Information.** DATA SHARING PARTNER may use Protected Health Information to perform data aggregation services for STATE. The use of Protected Health Information by DATA SHARING PARTNER to

perform data analysis or aggregation for parties other than STATE must be expressly approve by STATE.

6.5 STATE Data Responsibilities

- A. STATE shall disclose Protected Information only as authorized by law to DATA SHARING PARTNER for its use or disclosure.
- B. STATE shall obtain any consents or authorizations that may be necessary for it to disclose Protected Information with DATA SHARING PARTNER.
- C. STATE shall notify DATA SHARING PARTNER of any limitations that apply to STATE's use and disclosure of Protected Information that would also limit the use or disclosure of Protected Information by DATA SHARING PARTNER.
- D. STATE shall refrain from requesting DATA SHARING PARTNER to use or disclose Protected Information in a manner that would violate applicable law or would be impermissible if the use or disclosure were performed by STATE.

6.6 Obligations of DATA SHARING PARTNER Upon Expiration or Cancellation of this Agreement. Upon expiration or termination of this Agreement for any reason:

- A. DATA SHARING PARTNER shall retain only that Protected Health Information which is necessary for DATA SHARING PARTNER to continue its proper management and administration or to carry out its legal responsibilities, and maintain appropriate safeguards and comply with Subpart C of 45 C.F.R. Part 164 with respect to electronic Protected Health Information to prevent the impermissible use or disclosure of any retained Protected Health Information for as long as DATA SHARING PARTNER retains the Protected Health Information.
- B. For all other Protected Information, in compliance with the procedures found in the Applicable Safeguards listed in Section 6.1, or as otherwise required by applicable industry standards, or directed by STATE, DATA SHARING PARTNER shall immediately, destroy or sanitize (permanently de-identify without the possibility of re-identification), or return in a secure manner to STATE all Protected Information that it still maintains.
- C. DATA SHARING PARTNER shall ensure and document that the same action is taken for all Protected Information shared by STATE that may be in the possession of its contractors, subcontractors, or agents. DATA SHARING PARTNER and its contractors, subcontractors, or agents shall not retain copies of any Protected Information.
- D. In the event that DATA SHARING PARTNER cannot reasonably or does not return or destroy Protected Information, it shall notify STATE of the specific laws, rules or policies and specific circumstances applicable to its retention, and continue to extend the protections of this Agreement and take all measures possible to limit further uses and disclosures of the client data for so long as DATA SHARING

PARTNER or its contractors, subcontractors, or agents maintain the Protected Information.

- E. DATA SHARING PARTNER shall document and verify in a report to STATE the disposition of Protected Information. The report shall include at a minimum the following information:
 - 1. A description of all such information and the media in which it has been maintained that has been sanitized or destroyed, whether performed internally or by a service provider;
 - 2. The method by which, and the date when, the data and media were destroyed, sanitized, or securely returned to STATE; and
 - 3. The identity of organization name (if different than DATA SHARING PARTNER), and name, address, and phone number, and signature of individual, that performed the activities required by this Section.
- F. Documentation required by this Section shall be made available upon demand by STATE.
- G. Any costs incurred by DATA SHARING PARTNER in fulfilling its obligations under this Section will be the sole responsibility of DATA SHARING PARTNER.

7. Intellectual Property Rights.

- 7.1 **Definitions.** *Works* means all inventions, improvements, discoveries (whether or not patentable or copyrightable), databases, computer programs, reports, notes, studies, photographs, negatives, designs, drawings, specifications, materials, tapes, and disks conceived, reduced to practice, created or originated by Health, its employees, agents, and subcontractors, either individually or jointly with others in the performance of this Agreement. *Works* includes "*Documents.*" *Documents* are the originals of any databases, computer programs, reports, notes, studies, photographs, negatives, designs, drawings, specifications, materials, tapes, disks, or other materials, whether in tangible or electronic forms, prepared by Health, its employees, agents, or subcontractors, in the performance of this Agreement.
- 7.2 **[Option 1] Use of Works and Documents.** DATA SHARING PARTNER owns any Works or Documents developed by DATA SHARING PARTNER in the performance of this Agreement. STATE and the U.S. Department of Health and Human Services will have royalty free, non-exclusive, perpetual and irrevocable right to reproduce, publish, or otherwise use, and to authorize others to use, the Works or Documents for government purposes. If using STATE data, DATA SHARING PARTNER must cite the data, or make clear by referencing that STATE is the source.
- 7.2 **[Option 2] Ownership.** STATE owns all rights, title, and interest in all of the intellectual property, including copyrights, patents, trade secrets, trademarks, and service marks in the Works and Documents created under this Agreement. The Works and Documents

will be the exclusive property of STATE and all such Works and Documents must be immediately returned to STATE by DATA SHARING PARTNER upon completion or cancellation of this Agreement. To the extent possible, those Works eligible for copyright protection under the United States Copyright Act will be deemed to be “works made for hire.” If using STATE data, DATA SHARING PARTNER must cite the data, or make clear by referencing that STATE is the source.

8. **Indemnification.** DATA SHARING PARTNER agrees to indemnify, save and hold STATE, its representatives and employees harmless from any and all claims or causes of action, including all attorneys’ fees incurred by STATE, arising from the performance of this Agreement by DATA SHARING PARTNER or its agents or employees. This clause will not be construed to bar any legal remedies DATA SHARING PARTNER may have for STATE’s failure to fulfill its obligations pursuant to this Agreement. The liability of STATE is governed by the provisions of the Minnesota Tort Claims Act and Minnesota Statutes, section 3.736.

The parties acknowledge that if a party is in violation of this Agreement, or violation of a federal or state statute applicable to Protected Information, the other party may limit, suspend, or terminate the violating party’s access to or use of Protected Information.

9. **Severability.** If any provision of this Agreement is held unenforceable, then such provision will be modified to reflect the parties’ intention. All remaining provisions of this Agreement shall remain in full force and effect.

10. **Cancellation.** This Agreement may be canceled by STATE or DATA SHARING PARTNER at any time, with or without cause, upon thirty (30) days written notice to the other party. Notwithstanding the preceding sentence, STATE may cancel this Agreement immediately if DATA SHARING PARTNER has breached a material term of this Agreement.

10.1 **Cancellation for Lack of Contract Funding.** STATE may immediately terminate this Agreement if it does not obtain funding from the Minnesota Legislature, or other funding source; or if funding cannot be continued at a level sufficient to allow for the payment of the services covered here. Termination will be by written or fax notice to DATA SHARING PARTNER. STATE is not obligated to pay for any services that are provided after notice and effective date of termination. However, DATA SHARING PARTNER will be entitled to payment, determined on a pro rata basis, for services satisfactorily performed to the extent that funds are available. STATE will not be assessed any penalty if the Agreement is terminated because of the decision of the Minnesota Legislature, or other funding source, not to appropriate funds. STATE must provide DATA SHARING PARTNER notice of the lack of funding within a reasonable time of STATE receiving that notice.

10.2 **Cancellation for Breach.** STATE may immediately terminate this Agreement if DATA SHARING PARTNER is in material breach of this Agreement and STATE determines that cure of the breach is not possible. However, STATE may, in its discretion, allow DATA SHARING PARTNER to cure the breach or end the violation. If efforts to cure the breach or end the violation are not successful within the time period specified by STATE, STATE shall terminate this Agreement. If neither termination nor cure is feasible, STATE shall

report the violation to the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR).

- 11. Governing Law, Jurisdiction and Venue.** Minnesota law, without regard to its choice of law provisions, governs this Agreement, and amendments and supplements thereto. Without STATE waiving its sovereign immunity, venue for all legal proceedings arising out of this Agreement, or breach thereof, will be in the state or federal court with competent jurisdiction in Ramsey County, Minnesota.
- 12. Assignment, Amendments, Waiver, Endorsement and Agreement Complete.**
 - 12.1 Assignment.** The parties may neither assign nor transfer any rights or obligations under this Agreement without the prior consent of the other party and a fully executed Assignment Agreement, approved by the same parties who executed and approved this Agreement, or their successors in office.
 - 12.2 Amendments.** Any amendment to this Agreement must be in writing and will not be effective until it has been executed and approved by the same parties who executed and approved the original Agreement, or their successors in office.
 - 12.3 Waiver.** If either party fails to enforce any provision of this Agreement, that failure does not waive the provision or the party's right to enforce it.
 - 12.4 Endorsement.** DATA SHARING PARTNER must not claim that STATE endorses its products or services.
 - 12.5 Agreement Complete.** This Agreement contains all negotiations and Agreements between STATE and DATA SHARING PARTNER. No other understanding regarding this Agreement, whether written or oral, may be used to bind either party.
- 13. Interpretation.** Any ambiguity in this Agreement shall be resolved to permit the parties to comply with HIPAA, the Minnesota Government Data Practices Act, and other applicable state and federal statutes, rules, and regulations affecting the collection, storage, use and dissemination of private or confidential information.
- 14. Survival of Terms.** The rights and obligations of the parties under this Agreement shall survive the termination of this Agreement for as long as DATA SHARING PARTNER or its subcontractors and agents are in possession of Protected Information received from or collected, created, used, maintained, or disclosed on behalf of STATE. The duties and obligations of DATA SHARING PARTNER in Section 6.6 shall survive termination of this Agreement.
- 15. Insurance.**
 - 15.1 Commercial General Liability Insurance.** DATA SHARING PARTNER shall, at all times during the term of this Agreement, keep in force a commercial general liability insurance policy with the following minimum amounts: \$2,000,000 per occurrence and \$2,000,000 annual aggregate, protecting it from claims for damages for bodily injury, including sickness or disease, death, and for care and loss of services as well as from

claims for property damage, including loss of use which may arise from operations under this Agreement whether the operations are by DATA SHARING PARTNER or by a subcontractor or by anyone directly or indirectly employed by DATA SHARING PARTNER under this Agreement.

15.2 Professional/Technical, Errors and Omissions, and/or Miscellaneous Liability

Insurance. DATA SHARING PARTNER shall, at all times during the term of this Agreement, keep in force a professional/technical, errors and omissions, or miscellaneous liability insurance policy that will provide coverage for all claims the contractor may become legally obligated to pay resulting from any actual or alleged negligent act, error, or omission related to DATA SHARING PARTNER'S professional services required under this Agreement. DATA SHARING PARTNER is required to carry the following minimum limits under its professional/technical, errors and omissions, or miscellaneous liability insurance policy:

\$2,000,000 – per claim or event
\$2,000,000 – annual aggregate

Any deductible will be the sole responsibility of the Contractor and may not exceed \$50,000 without the written approval of the State. The retroactive or prior acts date of such coverage shall not be after the effective date of this Contract and Contractor shall maintain such insurance for a period of at least three (3) years, following completion of the work. If such insurance is discontinued, extended reporting period coverage must be obtained by Contractor to fulfill this requirement.

15.3 Network Security and Privacy Liability Insurance. DATA SHARING PARTNER shall, at all times during the term of this Agreement, keep in force a network security and privacy liability insurance policy. The coverage may be endorsed on another form of liability coverage or written on a standalone policy.

DATA SHARING PARTNER shall maintain insurance to cover claims which may arise from failure of DATA SHARING PARTNER's security resulting in, but not limited to, computer attacks, unauthorized access, disclosure of not public data including but not limited to confidential or private information, transmission of a computer virus or denial of service. DATA SHARING PARTNER is required to carry the following **minimum** limits:

\$2,000,000 per occurrence
\$2,000,000 annual aggregate

15.4 Privacy Liability Insurance. The DATA SHARING PARTNER shall maintain insurance to cover claims which may arise from failure of the DATA SHARING PARTNER to ensure the security of not public data stored on the State's documents, including but not limited to paper, microfilms, microfiche, magnetic computer tapes, cassette tapes, photographic negatives, photos, hard disks, floppy disks, and carbon sheets, while in the DATA SHARING PARTNER's care, custody, and control. The coverage may be endorsed on another form of liability coverage or written on a standalone policy. Contractor is required to carry the following **minimum** limits:

\$2,000,000 – Per Occurrence
\$2,000,000 – Annual Aggregate

- 15.5 Commercial Automobile Liability.** DATA SHARING PARTNER is required to maintain insurance protecting the responder from claims for damages for bodily injury as well as from claims for property damage resulting from ownership, operation, maintenance or use of all owned, hired, and non-owned autos which may arise from operations under this Agreement, and in case any work is subcontracted the responder will require the subcontractor to provide Commercial Automobile Liability. Insurance minimum amounts are as follows:

\$2,000,000 – per occurrence Combined Single limit for Bodily Injury and Property Damage

In addition, the following coverages should be included:

Owned, Hired, and Non-owned Automobile

- 16. Worker's Compensation.** DATA SHARING PARTNER certifies that it is in compliance with Minn. Stat. § 176.181, subd. 2, pertaining to workers' compensation insurance coverage. DATA SHARING PARTNER's employees and agents will not be considered employees of STATE. Any claims that may arise under the Minnesota Workers' Compensation Act on behalf of these employees or agents and any claims made by any third party as a consequence of any act or omission on the part of these employees or agents are in no way STATE'S obligation or responsibility.

- 17. Other Provisions.** Reserved.

**REMAINDER OF PAGE INTENTIONALLY LEFT BLANK.
(Signature Page Follows)**

IN WITNESS WHEREOF, the parties have caused this Agreement to be duly executed intending to be bound thereby.

APPROVED:

1. DATA SHARING PARTNER:

DATA SHARING PARTNER certifies that the appropriate person(s) have executed the Agreement on behalf of DATA SHARING PARTNER as required by applicable articles, by-laws resolutions or ordinances.

By: _____

Printed Name: _____

Title: _____

Date: _____

2. STATE:

By: _____

Printed Name: _____

Title: _____

Date: _____

Distribution (One fully executed original Agreement each):

Contracting, Procurement & Legal Compliance Division

Agency

DATA SHARING PARTNER

STATE Authorized Representative – (copy)

Appendix I: PHR Vendor Review of Requirements Documentation Statement



Minnesota Department of **Human Services**

As the contracted PHR vendor for the PHR Community Collaborative, we affirm that:

- We have thoroughly reviewed the requirements documentation,
- We are willing to participate in the project, and
- To the best of our knowledge, our technology solution is capable of meeting the RFP requirements (with exceptions clearly noted in our response to the Detailed Business Requirements Workbook).

Vendor Information

PHR Community Collaborative Name: _____

PHR Vendor Name: _____

Vendor Authorized Signature: _____

Printed Name: _____

Title: _____

Date: _____ Telephone Number: _____

ADA2 (12-12)

This information is available in accessible formats for individuals with disabilities by calling 651-431-3612 or by using your preferred relay service. For other information on disability rights and protections, contact the agency's ADA coordinator.