

10.0 PRIVACY AND SECURITY

Blueprint Application

November, 2012

10.1 Privacy and Security standards, policies, and procedures

10.2 Safeguards based on HHS IT guidance

10.3 Safeguard protections for Federal information

Description

The Minnesota Exchange views its obligation to protect citizens' data as one of its primary duties. In order to carry out this duty, the Exchange will implement strict privacy and security policies that meet all applicable state and federal requirements, including policies that put in place robust technical, physical, and administrative safeguards for data under the control of the Exchange.

The Exchange, in close cooperation with the Department of Human Services ("DHS") and the Office of Enterprise Technology (known as MN.IT Services - "MN.IT"), has begun the process of establishing a comprehensive privacy and security program that will use or leverage existing state agency policies, procedures and standards where applicable and, where no applicable policies, procedures, or standards are existing and available for use, create ones that are appropriate and effective to meet the unique privacy and security requirements of the Exchange.

The following are brief descriptions of the current and planned activities of the Exchange related to privacy and security:

1. The Exchange has identified the need for and is proceeding to fill an Exchange Privacy and Security Officer position to lead the development, implementation, and maintenance of privacy and security programs within the Exchange. To assist the Privacy and Security Officer, a consultant role of a project manager/ business analyst for data privacy and security certification has been created specifically for the development and implementation phase.
2. The Exchange has convened with a multi-agency Security and Privacy Governance Committee. This Committee has responsibility to assist the Exchange in the identification and/or creation, and implementation of standards, policies, and procedures to ensure the Exchange is in full compliance with the all privacy standards outlined in the final exchange regulations in 45 C.F.R. § 155.260(a) – (g). Additionally, the Committee serves as in an advisory role regarding data privacy and security related topics. To ensure the successful completion of its charge, the Privacy and Security Governance Committee will meet weekly with assigned work group leads, structured agendas and timelines, and access to appropriate resources to complete action items and tasks.
3. The Exchange, in collaboration with the Privacy and Security Governance Committee, is in the process of conducting a gap analysis which will identify the privacy and security standards, policies and procedures available within state agencies for the Exchange to use today, along with the identification of areas where new standards, policies or procedures may need to be created. Given that the Department of Human Services ("DHS"), as the state Medicaid agency, has a substantial base of policies and procedures related to privacy and security in place, an initial step in the gap analysis has been to identify how these DHS policies and procedures might be used or leveraged to

meet the federal requirements for privacy and security. Additionally, the Exchange will draft an overview of the applicability of various state and federal laws to data contained within the Exchange in order to determine which standards, policies and procedures may need to be applied to various types and classifications of data.

4. As the gap analysis is completed, the Exchange, in collaboration with the Privacy and Security Governance Committee, will begin developing and drafting those standards, policies, and procedures that are not currently in existence. Concurrently, the existing applicable standards, policies and procedures, along with any new standards, policies and procedures created, will be compiled into a comprehensive Exchange Privacy and Security Manual. This Manual will be published and updated on a regular basis.
5. The Exchange will develop and implement extensive communication and training plans to ensure all users of the Exchange, both internal to the Exchange organizational structure as well as external partners, receive appropriate training and information regarding all relevant privacy and security policies, procedures and standards. These plans will include the following:
 - a. Processes of delivery of training and communication to users;
 - b. Monitoring to assure proper delivery of training and communication; and
 - c. In conjunction with the Exchange oversight and monitoring program, monitoring training and communication to assure adhere to applicable policies.
6. Throughout the development of the Exchange Solution, the Exchange staff will work closely with the State staff and Contractor staff to ensure that all necessary privacy and security functionality is appropriately integrated into the Exchange Solution.

Minnesota Health Insurance Exchange Blueprint Application Documentation

Documentation

<u>Document</u>	<u>Description</u>
Business Process Models	The Enterprise end-to-end process models document the planned flow of Exchange functions necessary to meet federal and state requirements to support individuals, employees, employers, health plans, providers, and assisters.
MN technical infrastructure contract	<p>The Minnesota Health Insurance Exchange will leverage the technical infrastructure contract documents in support of evaluating, analyzing and bringing functionality to a level of operational readiness. Specific to <i>section 10.0 Privacy and Security</i>, the areas within the Contract referenced for this area are:</p> <p><i>Terms and Conditions</i></p> <p><i>Section 27</i></p> <p><i>Section 28</i></p> <p><i>Exhibit A – Business Functional Requirements</i></p> <p><i>Page 5, III.c.1</i></p> <p><i>Page 7, III.d.5</i></p> <p><i>Page 14, V.f.13</i></p> <p><i>Page 32, VIII.b.1.H.i</i></p> <p><i>Page 34, VIII.d.3.A.i</i></p> <p><i>Page 36, IX.a.4</i></p> <p><i>Page 37, IX.b.8</i></p> <p><i>Page 37, IX.c.1-7</i></p> <p><i>Page 38, IX.d.2,4-5</i></p> <p><i>Page 38-39, IX.f.6,8</i></p> <p><i>Page 39, IX.g.4</i></p> <p><i>Page 39, IX.h.1-5</i></p> <p><i>Exhibit B – Technical Requirements and Module Definition and Scope</i></p> <p><i>Page 1, II.a.5,13</i></p> <p><i>Page 3-4, II.b.8,17</i></p> <p><i>Page 9-10, II.f.15-19</i></p> <p><i>Page 15, II.k.4-8</i></p> <p><i>Exhibit D – Data Sharing Agreement</i></p>
IT Exchange Life Cycle Artifacts List for Federal compliance documentation	An informational guide to the mapping of the documented artifacts which are required in support of the formal review of the Establishment Process and the Medicaid IT Process.
Initial Gap Analysis Document	This document is an initial gap analysis of how existing DHS policies and procedures may be used or leveraged to meet federal requirements for the Exchange.
DHS Policies and Procedures Document	This document provides links to current DHS policies related to privacy and security that may be used or leveraged in to federal requirements for the Exchange

Open Policy Decisions (if applicable)

1. Whether to allow the Exchange access to other Minnesota state agency databases to perform additional data verifications for eligibility determinations or for other purposes.