DirectTrust Comments on Standard Operating Procedure (SOP): QHIN, Participant, and Subparticipant Additional Security Requirements

DirectTrust Community Response

Submitted Electronically: January 13, 2023

1 DirectTrust's Comments on Standard Operating Procedure (SOP): QHIN, Participant, and Subparticipant Additional Security Requirements – Section 5: Procedure

1.1 Feedback Regarding: The Selection of Authentication Assurance Levels (AAL)

DirectTrust generally agrees with the Authentication Assurance Levels (AAL) selected by the RCE for both workforce and individuals. However, the risk profiles of the workforce and the impact of selecting an AAL2 assurance level is not consistent across the workforce members that would be subject to this IG. The information below is offered as additional context to the RCE to make a risk-based decision concerning the appropriate AAL for workforce members by taking into consideration the various types of actors that may be impacted. It may be valuable to establish different expectations for different circumstances.

In principle, selecting any assurance level is a determination regarding the appropriate risk management. Risk management often observes three distinct, and sometimes competing, security objectives defined by FIPS 199: [1]

1. Confidentiality: Keeping data secret except to authorized parties

2. Integrity: Keeping data intact with provenance concerning it's origin; and

3. Availability: Access to data when needed.

NIST SP 800-63-3 defines a rather lengthy risk assessment process that is designed to determine the appropriate assurance level for a given system. Unfortunately, this IG encompasses many systems, which may make the guidance difficult to observe.

As a result, DirectTrust offers the following examples to illustrate the general approach to risk management using FIPS 199.

Example 1: A physician is authenticating to a healthcare system from an off-campus location that is also off the healthcare organization's network (no VPN).

1. Confidentiality: Keeping the healthcare data that the provider intends to access is a high-value objective.

[1] https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf

2. Integrity: Ensuring the integrity of the healthcare data that the provider intends to access is also a high-value objective.

3. Availability: While ensuring the data is available to access is also a high value objective, the speed in which the physician accesses the data (measured in seconds or minutes) is not as important at protecting confidentiality and integrity.

Result: AAL2 offers strong multi factor authentication which allows the data to be secured from a remote location, even if the authenticators may take longer to use than AAL1 authenticators. In such a circumstance, we believe AAL2 is an appropriate assurance level.

Example 2: A physician is authenticating to a healthcare system from an on-campus location or a location that is connected to the healthcare network (e.g. VPN) using strong authentication, where healthcare services are being administered to a patient.

1. Confidentiality: Keeping the healthcare data that the provider intends to access is a high-value objective.

2. Integrity: Ensuring the integrity of the healthcare data that the provider intends to access is also a high-value objective.

3. Availability: Both the availability of the data and immediate access to the data may be a very high-value objective. In some cases, this objective may be of higher value than confidentiality and integrity objectives if a patient's immediate health is in jeopardy.

Result: While AAL2 offers strong multi factor authentication, which allows the data to be secured, the increased time or physical interaction required to activate AAL2 multi factor authenticators could be observed as a higher risk than confidentiality and integrity. In such circumstances, DirectTrust recommends taking a close look at the risk profile to ensure AAL2 is appropriate. If AAL2 is still deemed appropriate by the RCE, then DirectTrust recommends publishing additional guidance concerning which authenticators defined in NIST SP 800-63B Section 5.1 are most appropriate when immediate access to the system is required by the workforce member. Cryptographic authenticators that indicate the physical presence of the physician should be given priority in these circumstances, such as those defined in sections: 5.1.6, 5.1.7, 5.1.8 and 5.1.9. The RCE should consider the use of biometrics as activation data used with a physical authenticator. The RCE should also consider suggesting authenticators that support NFC or Bluetooth in support of hands-free authentication.

Additionally, given the risk analysis above, DirectTrust believes AAL2 for individuals is appropriate.

1.2 Feedback Regarding: Audit

Participants and Subparticipants will often not be healthcare organizations and will often not be responsible for managing designated record sets. It is very reasonable to require these entities to record and archive audit logs for all transactions processed, including for each the date/time received and/or transmitted, a transaction identifier, the entity received from or sent to, and possibly other high-level information; however, it doesn't seem reasonable to require that organizations that are not Covered Entities and that are not responsible for managing a Designated Record Set store the entire transaction for a minimum of 10 years. Requiring this level of record keeping for such entities may actually increase the attack surface and risk of data breach of an individual's healthcare information by requiring that PHI be replicated and stored in multiple locations and for a lengthy period.

This comment relates to an excerpt from ASTM E2147 – 18 Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems[2]:

4.1 Data that document health services in health care organizations are business records and shall be archived to a secondary but retrievable medium, and readily accessible, such as data that would be archived in a server or cloud storage. Audit data shall be retained for as long as the medical record is maintained, and may not be destroyed before the medical record may legally be destroyed, and in any event, for at least 10 years or for two years after the legal age of majority, unless a longer period of record retention is prescribed by state, federal or other law or regulation.

[2] https://www.astm.org/e2147-18.html