Access Controls

June 2022

I. Introduction

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule requires covered entities (CE) and business associates (BA) to implement information system access controls as part of their technical safeguards. Access controls are technical policies and procedures for electronic information systems that maintain electronic protected health information (ePHI) to allow access only to those persons or software programs that have been granted access rights as specified in the Information Access Management standard of Security Rule's Administrative Safeguards.

The Access Control Standard has four implementation specifications. The first two are required and the last two are addressable:

1. Unique User Identification
2. Emergency Access Procedure;
3. Automatic Logoff; and
4. Encryption and Decryption.

II. Definitions

a. Access Controls: Policies and procedures for electronic information systems that maintain ePHI to allow access only to authorized users, programs, processes, or other systems.

b. Addressable: If an implementation specification is addressable, then the CE and BA must assess whether it is a reasonable and appropriate safeguard in the entity's environment. This involves analyzing the specification in reference to the likelihood of protecting the entity's ePHI from reasonably anticipated threats and hazards. If it is reasonable, then the CE or BA should implement. If the CE or BA determines it is not reasonable and chooses not to implement an addressable specification based on its assessment, it must document the reason and implement an equivalent alternative measure that accomplishes the same end. See 45 C.F.R. § 164.306(d)(ii)(B)(2) for more information.

c. Business Associate: A person or entity that creates, receives, maintains, or transmits protected health information (PHI) on behalf of a CE and is not considered a member of the CE workforce.

d. Covered Entity: Under HIPAA, this is a health plan, a healthcare clearinghouse, or a healthcare provider that conducts one or more covered transactions in electronic form.

e. Decryption: The use of an algorithmic process to transform encrypted data into a form that can be read and/or processed.
f. Electronic Protected Health Information: Individually identifiable health information that is transmitted by or maintained in electronic media.
g. Encryption: The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key. For the purposes of access controls, "encryption" is associated with the technical safeguards necessary to control access to ePHI during storage or transmission.
h. Protected Health Information (PHI): Individually identifiable health information created or received by a CE that relates to the past, present, or future physical or mental health of an individual and is transmitted or maintained in electronic, paper, or any other form. It excludes health information in employment records held by a CE in its role as an employer. PHI does not include health information of persons deceased more than 50 years.
i. Required: If an implementation specification is required, then a CE and BA must implement the implementation specification.
j. Risk Assessment: The process of analyzing threats to and vulnerabilities of an information system, and the potential impact resulting from the loss of information or capabilities of a system. This analysis is used as a basis for identifying appropriate and cost-effective security countermeasures.
k. Technical Safeguards: Technology and the policy and procedures for its use that protect electronic health information and control access to it.

III. Discussion

CEs and BAs have the responsibility to implement access controls that are appropriate for the role and/or function of each workforce member. While the HIPAA Security Rule does not specify a type of access control method or technology, the access controls should enable authorized users the rights and privileges to access the minimum necessary information needed to perform job functions.

There are four implementation specifications that make up the Access Controls standard:

a. **Unique User Identification**: The HIPAA Security Rule (45 C.F.R. § 164.312(a)(2)(i)), as implemented through DoDI 8580.02, requires organizations to assign a unique name and/or number for identifying and tracking user identity. Therefore, CEs and BAs must assign a unique name and/or number to each user within their organization. System processes will use this name and/or number to identify the user and associate the user with tracked actions taken by or on behalf of that user. Unique user identifiers ensure accountability by recording a user's actions to audit logs which can be reviewed for inappropriate access to ePHI and traced back to an individual user.

b. **Emergency Access Procedure**: The HIPAA Security Rule (45 C.F.R. § 164.312(a)(2)(ii)), as implemented through DoDI 8580.02, requires the establishment –

and implementation, as necessary – of procedures for obtaining necessary ePHI during an emergency. Hence, CEs and BAs must develop technical procedures and the associated documented instructions on how access to ePHI will be requested and/or obtained when normal methods for obtaining access fail due to a crisis situation. Two examples of situations that could potentially deny access to patient information stored in an automated information system include system failure and the unavailability of authorized users. CEs and BAs must develop procedures to grant temporary access to otherwise unauthorized providers when a patient's authorized providers are unavailable (such as during admission to a hospital Emergency Department). CEs and BAs should specify procedures for gaining access to information during a system emergency or failure as part of the security management plan.

c. **Automatic Logoff**: The HIPAA Security Rule (45 C.F.R. § 164.312(a)(2)(iii)), as implemented through DoDI 8580.02, calls CEs and BAs to assess the need to implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. This addressable specification means CEs and BAs should determine the need for and the strength of the automatic logoff through a risk assessment process. CEs and BAs should also evaluate the risk associated with information systems and assess the need for, and corresponding interval of, inactivity that would trigger a user's automatic logoff from a particular system. For example, a risk assessment might determine that the data in one information system is sensitive and set the automatic logoff to occur after five minutes of inactivity, while the data in a different system is not sensitive and automatic logoff period could be set for ten minutes. An equivalent measure that achieves inactivity lockout is allowed when an automatic logoff feature is determined to not be reasonable and/or appropriate. If an automatic logoff is not implemented, CEs and BAs must document the decision process and justification for their approach while addressing these controls in their risk management plan.

d. **Encryption and Decryption**: The HIPAA Security Rule (45 C.F.R. § 164.312(a)(2)(iv)), as implemented through DoDI 8580.02, focuses on the use of mechanism[s] to encrypt and decrypt ePHI. These mechanisms control access to ePHI at rest or in transit by only allowing those with the confidential key the ability access the data. Federal Information Processing Standards (FIPS) Publication 140-2 provides the encryption and decryption standards that must be followed. Encryption and decryption are an addressable specification which means that CEs and BAs should document and provide justification for their decision to implement encryption and decryption or, if implementing a mechanism is determined by a risk assessment to not be reasonable or appropriate, document why it is not reasonable or appropriate, implement an equivalent measure, and document how that alternative measure achieves the objective. The risk assessment should be based on the nature of the risk, the costs, and business environment of the CE and/or BA.

IV. Resources/References

45 C.F.R. § 164.306, Health Insurance Portability and Accountability act of 1996 (Security standards: General rules)

45 C.F.R §164.312, Health Insurance Portability and Accountability act of 1996 (Technical safeguards)

DoDI 8580.02, DoD Health Information Security Regulation, May 24, 2011

Security Requirements for Cryptographic Modules | NIST, March 22, 2019

If you have any questions about any of the information above, please contact the DHA PCLO at:
dha.ncr.admin-mgt.mbx.dha-privacyguidance@mail.mil