July 14, 2021

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Office for Civil Rights

Controlling Access to ePHI: For Whose Eyes Only?

Summer 2021 Cybersecurity Newsletter

A recent report of security incidents and data breaches found that 61% of analyzed data breaches in the healthcare sector were perpetrated by external threat actors and 39% by insiders.[1] Without appropriate authorization policies and procedures and access controls, hackers, workforce members, or anyone with an Internet connection may have impermissible access to the health data, including protected health information (PHI), that HIPAA regulated entities hold. News stories and OCR investigations abound of hackers infiltrating information systems, workforce members impermissibly accessing patients' health information, and electronic PHI (ePHI) being left on unsecured servers.

Information Access Management and Access Control are two HIPAA Security Rule standards that govern access to ePHI. These standards include several implementation specifications that are either required[2] or addressable.[3] HIPAA regulated entities must implement required implementation specifications. Addressable implementation specifications require HIPAA regulated entities to assess whether an implementation specification is a reasonable and appropriate safeguard in its environment, and if so to implement it. If a particular implementation specification is not reasonable and appropriate, entities must document why, and implement equivalent alternative measures if reasonable and appropriate.

Information Access Management is an administrative safeguard for ePHI and Access Control is a technical safeguard for ePHI. Although their roles in securing ePHI are distinct, together, they ensure that organizations implement policies and procedures and technical controls that limit access to ePHI to only authorized persons or software programs that have been granted access rights.

Information Access Management

The Information Access Management standard requires HIPAA covered entities and business associates to "implement policies and procedures for authorizing access to [ePHI] that are

[1] *See* https://enterprise.verizon.com/resources/reports/dbir/
[2] *See* 45 CFR 164.306(d)(2).
[3] *See* 45 CFR 164.306(d)(3).

consistent with the applicable requirements of [the HIPAA Privacy Rule]."[4] This standard has three implementation specifications, two of which have general applicability to covered entities and business associates (Access Authorization[5] and Access Establishment and Modification[6]) and the other which is specific to health care clearinghouses (Isolating Health Care Clearinghouse Functions[7]). While the Access Authorization and Access Establishment and Modification implementation specifications are similar, the former focuses on the policies for granting access to ePHI, whereas the latter focuses on the procedural aspects about how such access is established, documented, reviewed, and modified.

Access Authorization concerns the implementation of policies and procedures that govern how covered entities and business associates authorize or grant access to ePHI within their organization. This may include how access to each information system containing ePHI is requested, authorized, and granted, who is responsible for authorizing access requests, and the criteria for granting access. These policies typically govern the parameters for which individuals in particular workforce roles may be granted access to particular systems, applications, and data. Those parameters would reflect what information access is necessary for a workforce member to do their job. For example, a billing clerk role may not need access to medical images on a Pictures Archiving and Communication System (PACS) server in order to carry out their billing responsibilities.

Access Establishment and Modification policies describe how to establish, document, review, and modify a user's access to workstations, transactions, programs, or processes. For example, a workforce member being promoted or given some change in responsibility may require increased access to certain systems and decreased access to others. Another example is that a covered organization could change its system access requirements to permit remote access to systems containing ePHI during a pandemic. Policies and procedures should cover situations such as these to ensure that each workforce member's access continues to be appropriate for their role.

Access Control

The Access Control standard is a technical safeguard that requires covered entities and business associates to implement access controls for electronic information systems to allow access to ePHI only to those approved in accordance with the organization's Information Access Management process.[8] The flexible, scalable, and technology-neutral nature of the Security

[4] *See* 45 CFR 164.308(a)(4)(i), Standard: Information access management.
[5] 45 CFR 164.308(a)(4)(ii)(B), Implementation Specification: Access Authorization (Addressable).
[6] 45 CFR 164.308(a)(4)(ii)(C), Implementation Specification: Access Establishment and Modification (Addressable).
[7] 45 CFR 164.308(a)(4)(ii)(A), Implementation Specification: Isolating Health Care Clearinghouse Functions (Required).
[8] *See* 45 CFR 164.312(a)(1), Standard: Access Control.

Rule permits organizations to consider various access control mechanisms to prevent unauthorized access to ePHI. Such access controls could include role-based access, user-based access, attribute-based access, or any other access control mechanisms the organization deems appropriate.[9] Further, access controls need not be limited to computer systems. Firewalls, network segmentation, and network access control (NAC) solutions can also be effective means of limiting access to electronic information systems containing ePHI. Properly implemented, network-based solutions can limit the ability of a hacker to gain access to an organization's network or impede the ability of a hacker already in the network from accessing other information systems – especially systems containing sensitive data.

The Access Control standard includes four implementation specifications for limiting access to only authorized users and software programs. The first, Unique User Identification,[10] is a required implementation specification and is a key security requirement for any system, but particularly those containing ePHI. While the use of shared or generic usernames and passwords may seem to provide some short-term convenience, it severely degrades the integrity of a system because it removes accountability from individual users and makes it much easier for the system to become compromised. If information is improperly entered, altered, or deleted, whether intentionally or not, it can be very difficult to identify the person responsible (e.g., for training or sanctions) or determine which users may have been the victim of a phishing attack that introduced ransomware into the organization. Additionally, because shared usernames and passwords can become widely known, it may be difficult to know whether the person responsible was an authorized user. A former employee or contractor, a current employee not authorized for access, a friend or family member of an employee, or an outside hacker could be a source of unauthorized access. The inability to identify and track a user's identity due to the use of shared user IDs can also impede necessary investigations when the shared user ID is used for unauthorized or even criminal activity. For example, a malicious insider could take advantage of known shared user IDs to hide their activities when collecting personal medical and financial information to use for identity theft. In such as case, an organization's implemented audit controls would document the actions of the shared user ID, thus potentially limiting the organization's ability to properly identify and track the malicious insider.

The second implementation specification, Emergency Access Procedure,[11] is also a required implementation specification. This implementation specification is applicable in situations in which normal procedures for obtaining ePHI may not be available or may be severely limited, such as during power failures or the loss of Internet connectivity. Access controls are still necessary during an emergency, but may be very different from normal operations. For example, due to the recent COVID-19 public health emergency, many organizations quickly

[9] Health Insurance Reform: Security Standards; Final Rule, 68 Fed. Reg. 8334, 8355 (February 20, 2003).
[10] 45 CFR 164.312(a)(2)(i), Implementation Specification: Unique User Identification (Required).
[11] 45 CFR 164.312(a)(2)(ii), Implementation Specification: Emergency Access Procedure (Required).

implemented mass telework policies. How workforce members can securely access ePHI during periods of increased teleworking should be part of an organization's Emergency Access Procedures. Appropriate procedures should be established beforehand for how to access needed ePHI during an emergency.

The third implementation specification, Automatic Logoff,[12] is an addressable implementation specification. Users sometimes inadvertently leave workstations unattended for various reasons. In an emergency setting, a user may not have time to manually log out of a system. Implementing a mechanism to automatically terminate an electronic session after a period of inactivity reduces the risk of unauthorized access when a user forgets or is unable to terminate their session. Failure to implement automatic logoff not only increases the risk of unauthorized access and potential alteration or destruction of ePHI, it also impedes an organization's ability to properly investigate such unauthorized access because it would appear to originate from an authorized user.

The final implementation specification is Encryption and Decryption,[13] which is also an addressable implementation specification. This technical safeguard can reduce the risks and costs of unauthorized access to ePHI. For example, if a hacker gains access to unsecured ePHI on a network server or if a device containing unsecured ePHI is stolen, a breach of PHI will be presumed and reportable under the Breach Notification Rule (unless the presumption can be rebutted in accordance with the breach risk assessment described in 45 C.F.R. § 164.402(2)). The Breach Notification Rule applies to unsecured PHI which is PHI "that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under [the HITECH Act]."[14] OCR's *Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals*, which provides guidance for securing PHI, states that ePHI that is "at-rest" (i.e., stored in an information system or electronic media) is considered secured if it is encrypted in a manner consistent with NIST Special Publication 800-111 (*Guide to Storage Encryption Technologies for End User Devices*) (SP 800-111).

EPHI encrypted in a manner consistent with SP 800-111 is not considered unsecured PHI and therefore is not subject to the Breach Notification Rule. Encrypting ePHI in this manner is an excellent example of how implementing an effective encryption solution may not only fulfill an organization's encryption obligation under the Access Control standard, but also provides a means to leverage the Breach Notification Rule's safe-harbor provision.

As the use of mobile computing devices (e.g., laptops, smartphones, tablets) becomes more and more pervasive, the risks to sensitive data stored on such devices also increases. Many

[12] 45 CFR 164.312(a)(2)(iii), Implementation Specification: Automatic Logoff (Addressable).
[13] 45 CFR 164.312(a)(2)(iv), Implementation Specification: Encryption and Decryption (Addressable).
[14] 45 CFR 164.402.

mobile devices include encryption capabilities to protect sensitive data. Once enabled, a device's encryption solution can protect stored sensitive data, including ePHI, from unauthorized access in the event the device is lost or stolen.

Conclusion

Information Access Management and Access Control are complementary requirements of the Security Rule. Information Access Management defines how access to ePHI is authorized and Access Control implements technical controls to limit access to ePHI. The rise in data breaches due to hacking as well as threats to ePHI by malicious insiders highlight the importance of establishing and implementing appropriate policies and procedures regarding these Security Rule requirements. Ensuring that workforce members are only authorized to access the ePHI necessary and that technical controls are in place to restrict access to ePHI can help limit potential unauthorized access to ePHI for both threats.

Resources

Summer 2019 Cyber Security Newsletter: Managing Malicious Insider Threats:
https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-summer-2019/index.html

Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals:
https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html

Guide to Storage Encryption Technologies for End User Devices:
https://csrc.nist.gov/publications/detail/sp/800-111/final

** This document is not a final agency action, does not legally bind persons or entities outside the Federal government, and may be rescinded or modified in the Department's discretion.*