**U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES**

**Office for Civil Rights**

---

## August 2024 OCR Cybersecurity Newsletter

# *HIPAA Security Rule Facility Access Controls – What are they and how do you implement them?*

***Available online at https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-august-2024/index.html***

In today's environment of increased cyber-attacks and breaches of electronic protected health information (ePHI)[1] caused by hacking, malware, or ransomware, HIPAA covered entities[2] and business associates[3] (collectively, "regulated entities") may overlook the need for vigilance with regard to the physical security of their ePHI. When it comes to ensuring the confidentiality, integrity, and availability of ePHI, regulated entities must ensure that the physical security of their facilities is not neglected. Recent data security research suggests that only 7% of data security decision makers are concerned with breaches due to lost or stolen equipment, even though these account for 17% of breaches.[4] From 2020 through 2023, the Office for Civil Rights (OCR) received over 50 large breach reports (*i.e.*, breaches of unsecured protected health information (PHI) involving 500 or more individuals) affecting over 1,000,000 individuals attributable to stolen equipment and devices containing ePHI. Such equipment and devices were frequently described as being stolen during a burglary and included workstations, servers, laptops, external hard drives, backup devices, flash drives, smart phones, and medical devices. Regulated entities should ensure that they have proper physical safeguards, including Facility Access Controls, in place to deter and prevent unauthorized access.

A breach in the confidentiality of PHI due to stolen devices is not the only concern for protecting access to one's physical facilities. Loss of certain devices, such as servers that maintain patients' electronic medical records or medical devices that provide diagnostic or treatment services, could delay or impede delivery of health care. In their haste to flee with stolen equipment, criminals could also destroy physical structures or electronic components required for power or cooling for devices, or damage infrastructure required for network connectivity – all of which can introduce additional delays and costs to fully recover.

Implementing Facility Access Controls is analogous to securing your home. Prior to locking your home's entrances, you have not effectively secured your home; similarly, absent appropriate Facility Access Controls, you have not fully secured your ePHI. This newsletter provides an overview of important considerations for regulated entities when implementing the Facility Access Controls requirement of the HIPAA Security Rule.[5]

The Facility Access Controls standard of the HIPAA Security Rule requires that regulated entities "[i]mplement policies and procedures to limit physical access to [their] electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed."[6]

This standard consists of four addressable implementation specifications:[7] (1) contingency operations, (2) facility security plan, (3) access control and validation procedures, and (4) maintenance records. Each of these specifications are explained in more detail below. 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.[8] If a particular implementation specification is not reasonable and appropriate, regulated entities must document why, and implement an equivalent alternative measure if reasonable and appropriate.[9]

Securing facilities against potential opportunities for theft is only one aspect, albeit an important one, for regulated entities to consider when implementing Facility Access Controls. Another is providing physical access to systems and facilities in a secure manner during a disaster or emergency. Since 2018, HHS has issued waivers or modifications of certain HIPAA requirements under Section 1135 of the Social Security Act[10] 31 times.[11] Except for a waiver due to the COVID-19 public health emergency, all were issued because of natural disasters (*e.g.*, hurricanes, tornadoes, winter storms, wildfires) across the United States and its territories. Regulated entities may want to consider how increased risks of natural disasters and other emergencies could affect physical access to systems and facilities.

**A. Contingency Operations**

The Security Rule's administrative safeguards require a regulated entity to establish a contingency plan to respond to an emergency or other occurrence that damages systems containing ePHI.[12] Emergencies can include natural disasters such as floods or fires as well as human actions (e.g., malicious actions such as hacking and malware attacks as well as non-malicious actions such as an inexperienced system administrator accidentally disabling critical systems or deleting sensitive data). As OCR stated in previous rulemaking, "[a] contingency plan is the only way to protect the availability, integrity, and security of data during unexpected negative events. Data are often most exposed in these events, since the usual security measures may be disabled, ignored, or not observed."[13] Thus, contingency plans are critical to protecting the confidentiality, integrity, and availability of ePHI during unexpected adverse events. And by extension, contingency operations are critical to ensure access to facilities to support the execution of contingency plans.

If an entity needs to execute its contingency plans in response to a disaster or emergency affecting its physical facilities, it may also need to activate its contingency operations procedures. Contingency operations is an addressable implementation specification of the Facility Access Controls standard of the Security Rule.[14] Contingency operations are procedures established by regulated entities that provide for physical access to facilities to support execution of contingency plans and restoration efforts in the event of an emergency.[15]

The primary purpose of contingency operations is to maintain physical security and appropriate access to ePHI in support of data restoration activities. When developing contingency operations procedures, regulated entities could consider the following:

- Who requires access to facilities and ePHI during a disaster or emergency?
- Is there a process to provide expedited or temporary access to facilities and ePHI if needed?

- Are there alternate means to access facilities and ePHI?
- Is there a plan to monitor facilities (*e.g.*, assign workforce members, security guards) if safe to do so, or otherwise secure facility access points that may no longer be secure due to a disaster or emergency (*e.g.*, power outage, physical damage)?
- Who is responsible for the organization's contingency plans?
- Who is responsible for implementing the contingency plan for accessing facilities and ePHI in each department, unit, etc.?
- Are contingency plans established for various types of potential disasters and emergencies (*e.g.*, wildfire, flood, hurricane, tornado, earthquake, power outage, civil unrest, cyber incidents)?
- What activities, resources, and procedures are needed to carry out critical activities during prolonged interruptions to normal operations (*e.g.*, contracting for additional help to relieve workforce, contracting for fuel deliveries for generators during extended power outages)?

**B. Facility Security Plan**

The second addressable implementation specification of the Facility Access Controls standard is for regulated entities to establish a facility security plan.[16] The facility security plan is the implementation of policies and procedures of the regulated entity to protect its facilities and equipment from unauthorized physical access, tampering, and theft.[17] Each regulated entity has its own unique set of circumstances that will guide the development and implementation of its facility security plan. Within an entity, there may even be different facility security plans for different departments depending on each individual department's needs. When implementing its facility security plan, a regulated entity may consider reviewing its risk analysis to help guide it in determining the appropriate policies and procedures to include in the plan. Regulated entities that do not control the buildings they occupy or that share space with other organizations remain responsible for their own facility security plans. Further, it is important for a regulated entity to consider the facility security measures implemented by third parties in the regulated entity's facility security plan, since they impact the regulated entity's own facility security plan.[18]

When creating a facility security plan, regulated entities might consider how the following are integrated into such a plan: surveillance cameras; alarm systems; property control/inventory tags; employee/contractor ID badges and visitor badges; private security guards/patrols; facility escorts for visitors/contractors; and biometric, electronic, and/or mechanical security systems.

In addition, when creating a facility security plan, regulated entities could consider:

- training its workforce members on the facility security plan;
- conducting an annual review and update, as needed, of the facility security plan;
- designating a person to develop and implement the facility security plan; and
- testing the facility security plan to ensure it remains effective.

**C. Access Control and Validation Procedures**

The third *addressable implementation specification of the Facility Access Controls safeguard is access control and validation procedures, which is the* implementation of procedures to control and validate

access to facilities based on an individual's role or function, including visitor control and access to software for testing and revisions.[19] In other words, this implementation specification leads regulated entities to control who has physical access to facilities. Such procedures may vary among regulated entities depending on the nature of their facilities and operations. For example, some regulated entities may control contractor access by requiring sign-in and sign-out along with a workforce member escort. Others, following appropriate vetting, may permit contractor access through the use of electronic key cards to limit access only to areas to which the contractor is permitted.

Considerations when developing access controls and validation procedures can include:

- ensuring policies and procedures for controlling access account for various roles and groups including, for example, staff, contractors, visitors, volunteers, interns, non-staff providers, and probationary employees;
- determining and documenting access points in each facility;
- creating an inventory of information technology assets; and
- developing a plan to ensure equipment is monitored as necessary.[20]

**D. Maintenance Records**

The final *addressable implementation specification of the Facility Access Controls safeguard is documenting and retaining maintenance records, which is the* implementation of policies and procedures to document information about repairs and modifications made to the physical components of a facility related to security (*e.g.*, hardware, walls, doors, locks).[21] Implementing such procedures and retaining documentation can assist regulated entities in ensuring accountability and in maintaining an effective facility security plan.

Maintenance record policies and procedures may vary with the size and type of regulated entity. For example, a small health care provider's office with a single location may document maintenance records in a logbook whereas a larger multi-location health care provider may record its maintenance activities electronically in a database.

A regulated entity's maintenance records could document:

- date and time of repair/modification;
- description of repair/modification;
- location of repair/modification;
- reasons for repair/modification, including any related to a security incident;
- name of individual(s) responsible for performing the repair/modification;
- name of individual(s) that authorize the repair/modification;
- any follow-up or additional repair/modification required; and
- name of individual(s) responsible for overseeing the repair/modification (*e.g.*, security officer, maintenance supervisor).

**OCR Enforcement**

Failure to implement Facility Access Controls can lead to a breach of PHI and potential enforcement actions by OCR for such failures. As an example, OCR investigated Fresenius Medical Care Holdings, Inc. (FMC) for potential violations of the HIPAA Rules stemming from five separate breach incidents.[22] Three of those incidents, which affected the PHI of 366 individuals, involved equipment stolen from FMC's facilities. The ePHI involved included names, admission dates, days and times of treatments, dates of birth, Social Security numbers, telephone numbers, and addresses.

OCR's investigation found potential violations of the HIPAA Rules, including failure to conduct an accurate and thorough risk analysis; failure to implement a mechanism to encrypt and decrypt ePHI; failure to implement policies and procedures that govern the receipt and removal of hardware and electronic media; failure to implement policies and procedures to address security incidents; impermissible disclosure of ePHI; and **failure to implement policies and procedures to safeguard their facilities and equipment therein from unauthorized access, tampering, and theft**.

OCR resolved this investigation with a monetary settlement of $3.5 million, a resolution agreement, and corrective action plan that identified steps for FMC to take to resolve potential violations of the HIPAA Privacy and Security Rules and to protect ePHI.

**Conclusion**

In the face of ongoing, remote cyber-attacks, regulated entities should not overlook Facility Access Controls or relegate them to a "check the box" exercise. Also, as the United States continues to experience the effects of extreme weather and natural disasters,[23] regulated entities may want to consider whether their facilities are under increased environmental risks and, if so, review and update their Facility Access Controls to reflect these increased risks.[24] Facility security is a vital part of a regulated entity's overall security plan to protect PHI and should be considered holistically with an entity's overall cybersecurity plan and HIPAA compliance program. Effective Facility Access Controls not only provide for securing sensitive areas from unauthorized access but can also be a vital part of an entity's recovery efforts when used in conjunction with an entity's overall contingency planning process.

***Additional Resources:***

*HIPAA Security Series on Physical Safeguards:*

- https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf - PDF

*FTC Physical Security:*

- https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/physical-security

*Interagency Security Committee Guide to Creating a Security Access Plan:*

- https://www.cisa.gov/sites/default/files/publications/ISC-Facility-Security-Plan-Guide-2015-508.pdf - PDF

*NIST SP 800-66 Guide to Implementing the HIPAA Security Rule:*

- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-66r2.pdf - PDF

*CISA Cybersecurity and Physical Security Convergence:*

- https://www.cisa.gov/sites/default/files/publications/Cybersecurity%2520and%2520Physical%2520Security%2520Convergence_508_01.05.2021.pdf - PDF

* 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.

---

**Endnotes**

[1] EPHI is individually identifiable health information transmitted by or maintained in electronic media that identifies an individual or there is a reasonable basis to believe that the information can be used to identify an individual, that is created or received by a covered entity that relates to the past, present, or future physical or mental condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual. *See* 45 CFR 160.103 (definitions of "electronic protected health information" and "individually identifiable health information").

[2] *See* 45 CFR 160.103 (definition of "Covered entity").

[3] *See* 45 CFR 160.103 (definition of "Business associate"). *See also* Office for Civil Rights, HHS, "Fact Sheet on Direct Liability of Business Associates," (May 2019), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/factsheet/index.html

[4] Security Week. *Lost and Stolen Devices: A Gateway to Data Breaches and Leaks*. (October 2023). Available at https://www.securityweek.com/lost-and-stolen-devices-a-gateway-to-data-breaches-and-leaks/ .

[5] OCR administers and enforces the HIPAA Privacy, Breach Notification, Security, and Enforcement Rules at 45 CFR Part 160 and Part 164 Subparts A, C, D and E. The Security Rule establishes national standards to protect ePHI created, received, transmitted, or maintained by covered entities and their business associates. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of ePHI.

[6] 45 CFR 164.310(a)(1).

[7] *See* 45 CFR 164.306(d)(3).

[8] 45 CFR 164.306(d)(3)(i)-(ii)(A).

[9] 45 CFR 164.306(d)(3)(ii)(B).

[10] *See* https://aspr.hhs.gov/legal/1135-Waivers/Pages/1135-Waivers.aspx.

[11] *See* https://aspr.hhs.gov/legal/1135-Waivers/Pages/default.aspx.

[12] 45 CFR 164.308(a)(7).

[13] 68 Fed. Reg. 8334, 8351.

[14] 45 CFR 164.310(a)(2)(i).

[15] *See Id.*

[16] 45 CFR 164.310 (a)(2)(ii).

[17] *See Id*.

[18] *See* "Health Insurance Reform: Security Standards; Final Rule", 68 Fed. Reg. 8334, 8353 (February 20, 2003).

[19] *See* 45 CFR 164.310(a)(2)(iii).

[20] *See* Jeffrey A. Maron, Nat'l Inst. Of Standards and Tech., "Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule A Cybersecurity Resource Guide," (Feb. 2024), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-66r2.pdf - PDF .

[21] *See* 45 CFR 164.310(a)(2)(iv).

[22] *See* Office for Civil Rights, HHS, "Five breaches add up to millions in settlement costs for entity that failed to heed HIPAA's risk analysis and risk management rules," (2018), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/fmcna/index.html.

[23] *See* https://www.whitehouse.gov/ostp/news-updates/2023/11/09/fact-sheet-fifth-national-climate-assessment-details-impacts-of-climate-change-on-regions-across-the-united-states/ .

[24] *See* 45 CFR 164.316(b)(2)(iii) (The *Update* implementation specification of the *Policies and Procedures* standard requiring regulated entities to "[r]eview documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the [ePHI].").