E-BRIEF SERIES

Healthicity

Your Guide to the HIPAA Security Rule

CJ Wolf MD, CHC, CPC, CCEP, CIA

WHAT ARE ADMINISTRATIVE SAFEGUARDS?

HHS OCR tracks and publicly reports the top five issues in their investigated cases closed with corrective action. Administrative Safeguards have been in the top five identified issues for the last four years of the most recently reported data. They were number four on the list for the most recent three years and number three for the year before those.

When many people think of the HIPAA Security Rule (which applies to electronic PHI or e-PHI), they probably think about encryption and other technical safeguards, and they would be right and prudent to do so. But what about Administrative Safeguards? What are they, and how do they relate to the HIPAA Security Rule?

The Security Rule defines Administrative Safeguards as “administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity’s workforce in relation to the protection of that information.”

Administrative Safeguards comprise over half of all the HIPAA Security requirements. They are important. In fact, the administrative safeguards are, in a way, the foundation of a HIPAA Security program.

> The Security Rule defines Administrative Safeguards as “administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information...”

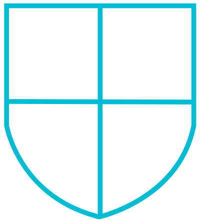
ACCORDING TO THE OCR, THE ADMINISTRATIVE SAFEGUARDS INCLUDE, BUT ARE NOT LIMITED TO:

- **Security Management Process:** A covered entity must identify and analyze potential risks to e-PHI. It must implement security measures that reduce risks and vulnerabilities to a reasonable and appropriate level.
- **Security Personnel:** A covered entity must designate a security official responsible for developing and implementing its security policies and procedures.
- **Information Access Management:** Consistent with the Privacy Rule standard limiting uses and disclosures of PHI to the “minimum necessary,” the Security Rule requires a covered entity to implement policies and procedures for authorizing access to e-PHI only when such access is appropriate based on the user or recipient’s role (role based access).
- **Workforce Training and Management:** A covered entity must provide appropriate authorization and supervision of workforce members who work with e-PHI. A covered entity must train all workforce members regarding its security policies and procedures and must have and apply appropriate

sanctions against workforce members who violate its policies and procedures.

- **Evaluation:**
  A covered entity must perform a periodic assessment of how well its security policies and procedures meet the requirements of the Security Rule.

All of these safeguards are essential, but two of the most important are the Security Management Process and Evaluation. That's why they're often included in what's often called a HIPAA Security Risk Analysis or HIPAA Security Risk Assessment and Management Plan.



HIPAA RISK ANALYSIS

A HIPAA Security Risk Analysis specifically assesses compliance with the HIPAA Security Rule. It is akin to a home inspection before a buyer closes the purchase of a home. The home inspection is an overall assessment of the home's structural stability, electrical systems, plumbing, roof, heating/air conditioning, and even integrity of the home's foundation. Some items in a home inspection need to be addressed immediately, while others can be planned over weeks or months. Similarly, a HIPAA risk analysis should look at all aspects of the overall HIPAA Security program and identify areas that need immediate improvement while prioritizing corrective action for other identified gaps.

When the OCR performed their nationwide audits, they identified some severe issues with entities' performance of a risk analysis. They found that only 31% of covered entities/business associates were substantially fulfilling their regulatory responsibilities to safeguard the e-PHI they hold through risk analysis activities. This means 69% were significantly noncompliant or not compliant at all.

The audits concluded that most entities generally failed to:

- Identify and assess the risks to all e-PHI in their possession.
- Develop and implement policies and procedures for conducting a risk analysis.
- Identify threats and vulnerabilities, consider their potential likelihoods and impacts, and rate the risk to e-PHI.
- Review and periodically update a risk analysis in response to changes in the environment and/or operations, security incidents, or the occurrence of a significant event.
- Conduct risk analyses consistent with policies and procedures.

WORKFORCE TRAINING: A VITAL ADMINISTRATIVE SAFEGUARD

Another vital administrative safeguard is workforce training. Many HIPAA Security Officials will tell you that most breaches or other non-compliance with the Security Rule result from human error. In other words, technical safeguards, once implemented, rarely fail. For example, if a laptop is appropriately encrypted, the encryption rarely fails. However, even if an organization has excellent technical safeguards in place, a workforce member could click on a link in a phishing email or allow a bad actor access to an organization's IT system in some other way. No number of technical safeguards can prevent bad results from human error.

Training employees is usually the best way to address this risk. And training an individual for a few hours upon initial hire isn't going to be enough. A good practice is to send "white hat" phishing email tests throughout the organization periodically while providing timely feedback to those who fail the test so they can learn, over time, the types of phishing attacks they might see in reality.

ADMINISTRATIVE SAFEGUARDS AS THE FOUNDATION OF YOUR HIPAA SECURITY PROGRAM

View administrative safeguards as the foundation of an organization's HIPAA Security program. They represent more than half of the HIPAA Security requirements. Before jumping into the Technical or Physical Safeguards, take a thoughtful approach to address the rule's Administrative Safeguards. Beginning with a HIPAA Security Risk Analysis and subsequent Management Plan is probably the best place to start.

PROTECTING PHI THROUGH PHYSICAL SAFEGUARDS

Has your organization ever terminated an employee? Did you have a procedure to collect that employee's keys and badge so they couldn't easily gain physical access to your organization and its PHI? Most likely, you can answer yes to all of these questions. These are examples of steps to protect PHI through physical safeguards.

THE $200,000 SETTLEMENT

One covered entity paid HHS Office for Civil Rights (OCR) a settlement of over $200,000 because, in part, it failed to follow through on these kinds of physical safeguards. According to the OCR's investigation, the covered entity terminated an employee during her probationary period. Eight days later, the former employee and a union representative entered the covered entity's offices. Using her work key, the former employee entered her old office and locked herself and the union representative inside. While inside the office, the former employee logged into her old computer with her username and password and downloaded information off her computer onto a USB drive. The former employee removed boxes containing personal items and paper documents. This was witnessed by a student intern who was present at the time. The former employee and the union representative then both exited the building.

These actions resulted in the impermissible disclosure of nearly 500 individuals' PHI. Would these things have happened if the organization had taken the former employee's work key? Though other failures occurred, such as not terminating the employee's computer login credentials, it's likely that if the physical security of the premises had been tighter, the former employee and union representative would not have been able to gain physical entry into the offices, preventing these other actions from taking place.

WHAT ARE PHYSICAL SAFEGUARDS?

The Security Rule defines physical safeguards as "physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion."

HHS has stated that when evaluating and implementing these standards, a covered entity must consider all physical access to ePHI. This may extend outside of an actual office and include workforce members' homes or other physical locations where they access ePHI.

It is difficult enough to physically secure an organization's headquartered offices and facilities. Consider, for example, all the healthcare workers who worked from home during the pandemic. Were their workstations physically secured? If they printed documents at home that contained PHI, did they have a mechanism to physically keep those documents secure? Some of these requirements are Security Rule requirements, while others might be Privacy Rule requirements, but the concept of physical safeguards, in general, helps protect PHI or electronic PHI (ePHI)

FACILITY ACCESS CONTROL

An important standard of the Physical Safeguards Requirement is Facility Access Controls. It requires covered entities to "Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed while ensuring that properly authorized access is allowed."

In regard to this first physical safeguard standard consider:

- Whether your organization's policies and procedures address allowing authorized and limiting unauthorized physical access to electronic information systems and equipment?
- Whether the policies and procedures identify individuals (workforce members, business associates, contractors, etc.) with authorized access by title and/or job function?
- Whether the policies and procedures specify the methods used to control physical access, such as door locks, electronic access control systems, security officers, or video monitoring?

"The term "electronic media" encompasses "electronic storage media including memory devices in computers (hard drives) and any removable/ transportable digital memory media, such as magnetic tape or disk, optical disk, or digital memory card...."

WORKSTATION AND DEVICE SECURITY

Another crucial physical safeguard standard is workstation and device security.

This standard requires entities to "Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information, into and out of a facility and the movement of these items within the facility."

The term "electronic media" encompasses "electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory media, such as magnetic tape or disk, optical disk, or digital memory card...."

Does this sound a little bit like herding cats? It sure can feel like it. Think about all the portable USB flash drives, laptop computers, electronic tablets, and phones that probably contain ePHI. Think about how they're moving in and out of facilities frequently to homes, coffee shops, parks, and little league games. Think about keeping track of all those moving pieces all the time. This is why some organizations decide to only allow ePHI on certain types of devices. For example, they may disable USB ports on computers so individuals cannot download any information onto unauthorized, portable flash drives.

Some questions to ask about this standard may include:

- Do your organization's policies and procedures govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility and the movement of these items within the facility?
- Do the policies and procedures identify the types of hardware and electronic media that must be tracked?
- Have all types of hardware and electronic media that must be tracked been identified, such as hard drives, magnetic tapes or disks, optical disks, or digital memory cards?

> "Other issues not addressed in this eBrief include the physical disposal of devices containing ePHI, re-use of devices containing ePHI, data backup and storage, contingency operations, facility security plan, access control/validation procedures, and maintenance records. It's a lot to consider."

FURTHER EXAMINATION

The Physical Safeguards requirements are more comprehensive than this current document can address. Other issues not addressed in this eBrief include the physical disposal of devices containing ePHI, re-use of devices containing ePHI (think re-purposing laptops or other equipment), data backup and storage, contingency operations, facility security plan, access control/validation procedures, and maintenance records. It's a lot to consider. And it's crucial to stay informed and in front of it all. Addressing the physical security of locations and equipment where ePHI is housed is essential to your overall HIPAA Security compliance program.

FIVE MILLION DOLLAR SETTLEMENT

A covered entity paid over $5 million to settle with HHS OCR over ePHI breach concerns and violations of the HIPAA Security Rule. OCR's investigation uncovered many concerns and among them were violations of the Technical Safeguards of the Security Rule. Some of these included the requirement to:

- Implement procedures to regularly review records of information system activity.
- Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights.
- Prevent unauthorized access to the ePHI of 9,358,891 individuals whose ePHI was maintained in the covered entity's IT systems.

WHAT ARE TECHNICAL SAFEGUARDS?

The Security Rule defines technical safeguards as "***the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.***"

Interestingly, the Security Rule does not specify specific technology solutions. HHS does provide some examples of security measures and technical solutions to illustrate the standards and implementation specifications. But these are only examples. There are many technical security tools, products, and solutions that a covered entity may select. As written by HHS, "Determining which security measure to implement is a decision that covered entities must make based on what is reasonable and appropriate for their specific organization, given their own unique characteristics..."

There are a lot of bad actors out there. Covered entities have seen a significant increase in hacking incidents. In fact, if you visit the OCR's list of breaches affecting over 500 individuals (see **https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf**) and scroll through that list, you will see "Hacking/IT Incident" as the most prominent type of breach listed for the most recent entries. Combating hackers will require a strong focus on both the technical safeguards and administrative safeguards primarily.

ACCESS CONTROL

ePHI is special information. Access to it is needed for physicians to write an order, for a nurse to enter notes and for a payor to process claims. Certain authorized individuals and technical systems need access to the information. Access to ePHI for legitimate purposes must be balanced with its security and prevention of unauthorized access.

The Security Rule defines access as "*the ability or the means necessary to read, write, modify, or communicate data/ information or otherwise use any system resource.*"

Reading, writing, modifying, and communicating are the life blood activities of medical records and payment systems. Controlling who has access to these activities is an essential technical safeguard.

Access controls provide users with rights and/or privileges to access and perform functions using information systems, applications, programs, or files. Levels of controls are also important. Not every authorized individual need full access to all ePHI content or systems. Controls should be implemented in a way that users only have access to the minimum necessary information needed to perform job functions. Rights and/or privileges should be granted to authorized users based on a set of access rules that the covered entity is required to implement as part of the Administrative Safeguards section of the Rule.

The Access Control standard requires a covered entity to:

"Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights..."

Some questions an organization may want to ask in relation to Access Controls include:

- Does each workforce member have a unique user identifier?
- What is the current format used for unique user identification?
- Can the unique user identifier be used to track user activity within information systems that contain ePHI?
- Do current information systems have an automatic logoff capability?
- Is the automatic logoff feature activated on all workstations with access to EPHI?

ENCRYPTION

Encryption falls under the Access Control standards as well. However, emphasizing encryption as a separate section in the eBrief is appropriate as the number of impermissible disclosures would be significantly reduced if organizations thoroughly and correctly implemented encryption best practices.

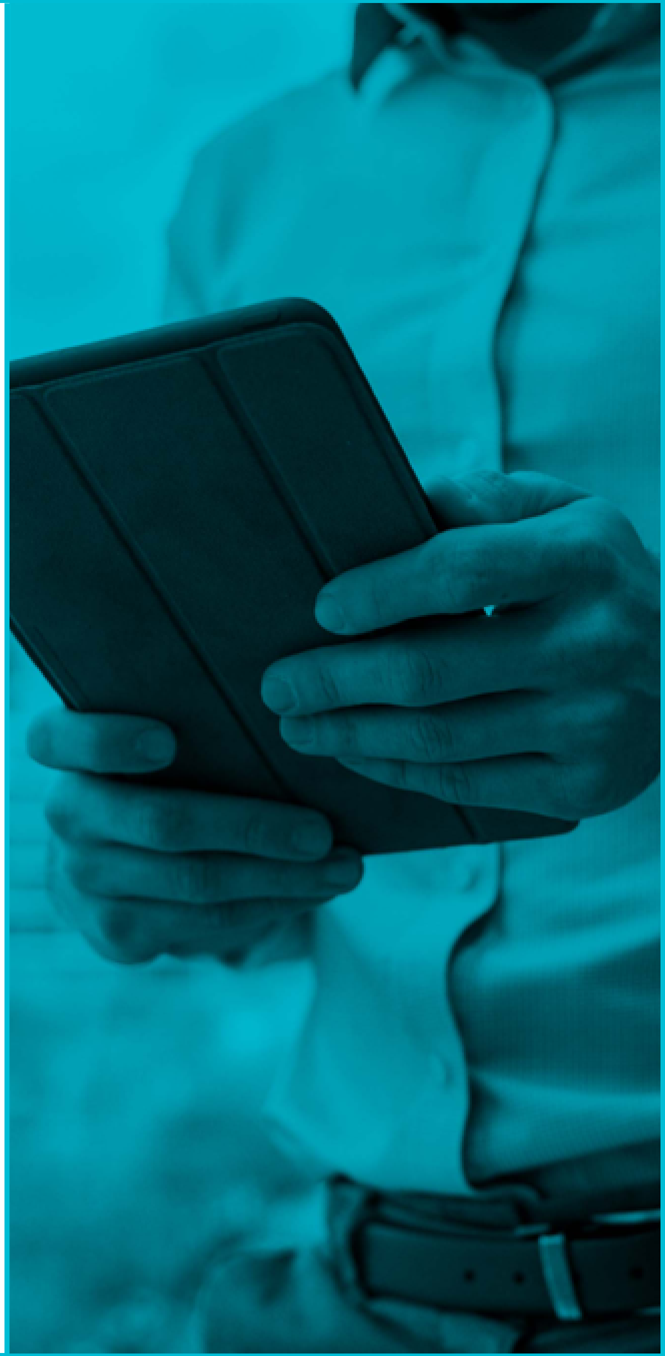
In fact, HHS has stated, "If information is encrypted, there would be a low probability that anyone other than the receiving party who has the key to the code or access to another confidential process would be able to decrypt (i.e., translate) the text and convert it into plain, comprehensible text."

Think of all the lost or stolen laptops or portable flash drives that contained ePHI. If you review the impermissible disclosures tracked by OCR, you will see how often a lost or stolen device is at the heart of a breach. If these lost or stolen devices had been properly encrypted, there essentially would have not been a reportable breach, as the probability of impermissible disclosure would have been close to zero because of the strength of proper encryption.

Regarding encryption, organizations might consider asking themselves:

- Which ePHI should be encrypted and decrypted to prevent access by persons or software programs that have not been granted access rights?
- What encryption and decryption mechanisms are reasonable and appropriate to implement to prevent access to ePHI by persons or software programs that have not been granted access rights?

The bottom line on encryption? Proper encryption would prevent significant numbers of impermissible disclosures. This is primarily true because historically such a large number of breaches were due to lost or stolen, unencrypted devices.



FAILURE CAN COST YOU

An orthopedic clinic in Georgia agreed to pay $1,500,000 to the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) and to adopt a corrective action plan to settle potential violations of the HIPAA Privacy and Security Rules.

The issue began when a hacker contacted the clinic and demanded money in return for a complete copy of the database they had stolen. The clinic determined that the hacker used a third-party vendor's credentials to access their electronic medical record system and exfiltrate patient health data. The hacker continued to access protected health information (PHI) for more than a month.

The OCR's investigation discovered longstanding systemic noncompliance with the HIPAA Privacy and Security Rules by the orthopedic clinic, including failures to conduct a risk analysis and implement risk management controls.

RISK ANALYSIS — OCR NATIONWIDE AUDIT RESULTS

Unfortunately, this clinic is like many other entities who are required to follow the HIPAA Security Rule. They often fail to perform an enterprise risk analysis and implement a risk management plan. In fact, when the OCR performed their nationwide audit of a sample of entities required to follow the HIPAA Security Rule, they found that only small percentages of covered entities (14%) and business associates (17%) were substantially fulfilling their regulatory responsibilities to safeguard electronic PHI (ePHI) they hold through risk analysis activities.

Some of the common errors the OCR found included failure to:

- Identify and assess the risks to all the ePHI in their possession.
- Develop and implement policies and procedures for conducting a risk analysis.
- Identify threats and vulnerabilities to consider their potential likelihoods and impacts and to rate the risk to ePHI.
- Review and periodically update a risk analysis in response to changes in the environment and/or operations, security incidents, or occurrence of a significant event.
- Conduct risk analyses consistent with policies and procedures.

Sometimes entities fail to comprehend their individual accountability to perform an enterprise risk analysis. They may mistakenly believe that an electronic medical records vendor or their contracted IT services are primarily responsible. This is not the case. In their audit, when the OCR requested documentation of an entity's HIPAA security risk analysis, providers commonly submitted documentation of some security activities of a third-party security vendor, but no documentation of any risk analysis. Or, in some cases, entities offered third-party template policy manuals that contain no evidence of entity-specific review or revision and no evidence of implementation.

RISK MANAGEMENT--OCR NATIONWIDE AUDIT RESULTS

Unfortunately, many entities feel that they are done once they've performed a HIPAA Security Risk Analysis. Though that step is essential, it is only the beginning. Once risks have been identified, they must be managed. Managing some risks might be more urgent than others. Prioritizing and developing a management plan, or project management plan, which identifies the steps the entity will take to mitigate the identified risks is the next step after the risk analysis is complete.

In regard to risk management steps, HHS has stated, "Risk management, required by the Security Rule, includes the implementation of security measures to reduce risk to reasonable and appropriate levels to, among other things, ensure the confidentiality, availability, and integrity of ePHI, protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI, and protect against any reasonably anticipated uses or disclosures of ePHI that are not permitted or required under the HIPAA Privacy Rule."

The OCR's audit results demonstrated that 94% of covered entities and 88% of business associates failed to implement appropriate risk management activities sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

Some of the key findings included:

- Entities lacked the necessary focus on technical safeguards (access controls, audit controls, etc.) needed to properly protect the confidentiality, integrity, and availability of ePHI.
- The policies and procedures provided in support of the risk analysis and risk management requirements indicate entity misunderstanding of the importance of determining acceptable levels of risk, what specific vulnerabilities were applicable to their environment, or how to mitigate the risks or vulnerabilities to ePHI throughout their organization.
- In some instances, encryption was included as part of a remediation plan, but was not carried out or was not implemented within a reasonable timeframe.
- One entity had implemented an appropriate risk management plan a few years earlier but failed to conduct any updates since that time.

> "The OCR's audit results demonstrated that 94% of covered entities and 88% of business associates failed to implement appropriate risk management activities sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level."

CONCLUSION

The bedrock foundation of a HIPAA Security compliance program is regular performance of an appropriate HIPAA Security risk analysis and development of a management plan. There have been numerous settlements with OCR when entities have not completed these requirements. In one OCR settlement, where the entity paid $3.5 million, the OCR director stated, "...there is no substitute for an enterprise-wide risk analysis for a covered entity." Indeed, there is no substitute.

"...there is no substitute for an enterprise-wide risk analysis for a covered entity."

-OCR Director

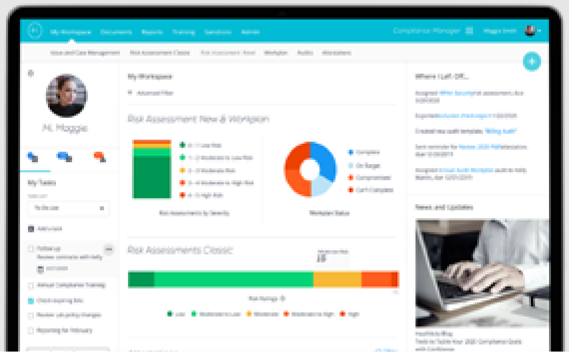
CJ Wolf

MD, CHC, CPC, CCEP, CIA

CJ Wolf is a healthcare professional with more than 25 years of experience in hospital and physician revenue cycle, practice management, compliance, coding, billing, and client services. He has provided healthcare consulting and solution services to hospitals and physician organizations throughout the country.

For more on Healthicity's Compliance Services and Solutions, please visit healthicity.com/compliance or call 877.777.3001

COMPLIANCE MANAGER



WATCH ON-DEMAND DEMO

RESOURCE CENTER

How To Effectively Communicate Compliance Reports

By Brenda Chidester-Palmer, CPC, CPC-I, CCS-P

EXPLORE FREE RESOURCES