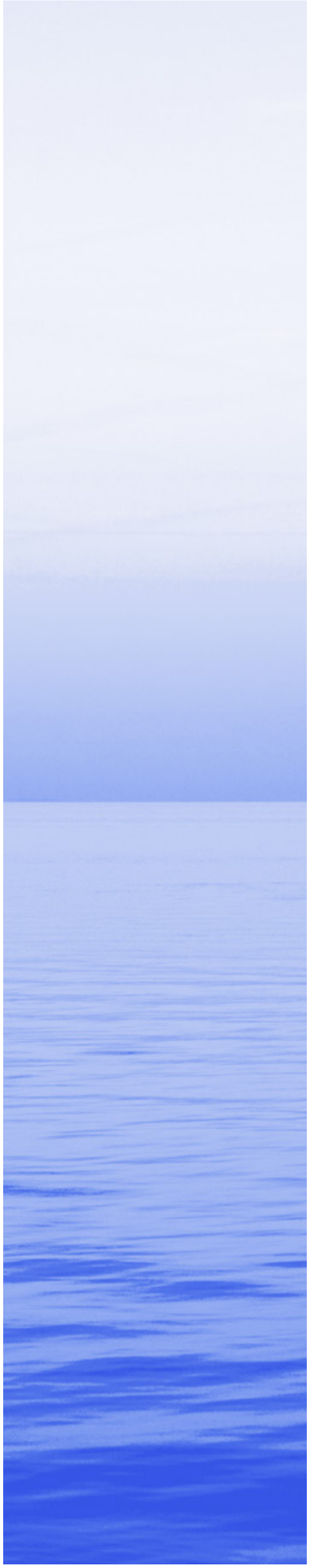
Clearwater

Whitepaper

How to Make System Activity Reviews an Effective Part of Your Security Program

Table of Contents

Introduction



As a covered entity or business associate, the Health Insurance Portability and Accountability Act (HIPAA) requires your organization establish procedures and controls to secure electronic protected health information (ePHI).

HIPAA's Security Rule dictates that if you handle ePHI, your organization must implement administrative safeguards to establish and maintain ePHI security. HIPAA 45 C.F.R. §164.308(a)(1)(ii)(D), for example, requires information system activity reviews to routinely analyze information system activity records including (but not limited to):

- Audit logs
- Access reports
- Security incident tracking reports

The goal is to protect ePHI and help your organization identify if ePHI has been reviewed, used, or disclosed inappropriately and then take steps to prevent further unauthorized disclosure. It establishes processes to monitor login attempts and report discrepancies.

HIPAA's technical safeguards also outline audit controls for all hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

Coupled with recommendations from NIST 800-53 and FIPS 199 and FIPS 200, you can develop a security program with clear guidelines about audit review, analysis of discovery, and reporting. These controls can be used to set your minimum security standards and then mature your program over time.

Understanding system activity reviews

According to the U.S. Department of Health and Human Services' Office for Civil Rights (OCR), organizations that handle ePHI must implement processes to regularly review system access activity records such as audit logs, access reports, and security incident tracking reports.

Here's a simpler way to look at it: Information system activity reviews are evaluations of your software and hardware activity logs, and you should conduct these reviews on a regular basis and compare it to your baseline information to discover, mitigate, and fix any potential security issues.

> A comprehensive system activity review (SAR) should always include your security, compliance, and privacy team members.

Setting the foundation with baseline information

Your system activity review processes should begin with an understanding of your baseline process and content. By establishing a baseline, you get insight into what normal or standard ePHI-related activities look like within your organization.

After documenting your baseline, as you build out your system activity review processes, you can refer to it to check for any potential gaps or processes that could impact your ability to detect anomalous activities. Be sure to include your compliance and privacy team members in this process. It helps ensure you're conducting a comprehensive review and will build inclusion so all of your core team members have a stake in your program.

What's a content review?

As part of your system activity review, it's important to understand what a content review is and what it includes. A content review includes a comprehensive review of all of your:

- User access logs
- User account
- Login time(s) and location
- Failed login attempts
- User access log modifications and deletions

- Record view logs
- Access logs of sensitive files, records, applications, or services

Here's an example:

Let's say your system administrator has access to all of your systems with ePHI. Of course, you'd hope that your administrators would never do anything nefarious or suspect, but it happens.

In 2013, for example, five employees and a research assistant at Cedars-Sinai Medical Center in Los Angeles were terminated after inappropriately reviewing patient records for celebrities, including reality TV personality Kim Kardashian, who had a child at the hospital the previous month. A similar breach happened in 2019, when 50 employees at Northwestern Memorial Hospital in Chicago lost their jobs after inappropriately accessing medical records for actor Jussie Smollett.

While these are examples of internal threats, ePHI isn't just at risk from the inside. In 2020 during the coronavirus pandemic, there's been a tremendous uptick in cyberattacks for healthcare organizations. A system activity review can help your organization spot, stop, and mitigate unauthorized ePHI access such as this.

Who needs system activity review?

In the first five months of 2020 alone, nearly 30 health systems reported data breaches ranging from malware and email phishing scams to inappropriate access of patient records. By early September 2020, the number of reported breaches under investigation by OCR already exceeded 300.

The reality is the healthcare threat landscape is intense, and if your organization handles ePHI, it's your responsibility to protect it. It's no longer about if a breach may occur, but for many organizations, it's when.

An effective system activity review can help your organization prevent or swiftly react to any malicious actions, which is paramount for an effective security program.

According to IBM's Cost of a Data Breach Report for 2020, the healthcare industry has the highest industry average cost of data breaches, topping more than $7 million. And per the same IBM report, it takes healthcare organizations an average of 329 days to discover and contain a data breach. So think of it like this: Your system activity review processes help stop the bleeding. Effective system activity review processes can lessen the amount of time that malicious actions can take place or even happen at all.

Which systems need activity reviews?

Think of your system activity review processes as it relates to your organizational risk analysis. If a system or application creates, receives, or maintains ePHI, it should be subject to a review.

Here are some examples:

- Network infrastructure
    - Routers, switches, firewalls (software and hardware), etc.
- Application servers
    - .NET, PHP, etc.
- Database servers
    - Microsoft SQL Server, Oracle, SAP HANA, etc.
- Physical devices (operating systems are immaterial here)
    - Desktops, laptops, portable electronic devices (PEDs), physical servers, etc.
- Virtual machines
    - Process and system
- Automated scheduled tasks and procedures
    - Scripts, reports, etc.
- Vendor products or services
    - SaaS, PaaS, IaaS, DaaS, etc.

It's important here to also point out if you work with a third-party vendor or supplier and that supplier creates, accesses, transmits or stores ePHI, you're still responsible for that ePHI. If you are a covered entity, you're responsible for the actions and activities of your business associates, so it's important to know what those externally hosted environments do and what they're protections are. But business associates are not exempt from this liability. If the business associate also uses a third-party vendor (known as a subcontractor) and that vendor creates, accesses, transmits or stores the ePHI, the business associate is responsible for the actions of the vendor.

Building comprehensive and inclusive processes

System activity reviews help covered entities and business associates proactively identify potential data breaches or anomalous or malicious activities.

However, because every covered entity and business associate has unique requirements and hierarchies, you should adopt an integrated approach to your system activity review program—one that includes IT, security, privacy, and compliance team members.

Your goal here is to build comprehensive and inclusive processes that keep your ePHI safe and reduce or eliminate common silos that often exist between functions for various business units and departments.

System activity review responsibilities

While your system administrators are responsible for coordinating and maintaining data sources (feeds or logs), because of a potential conflict of interest, those administrators should not perform activity reviews.

And while the responsibility to maintain those logs rests with your administrators, everyone on your team—including third-parties, for example your security operations center (SOC) if operated by an outside party—is a sensor responsible for reporting anomalous activities.

Although these team members aren't responsible for conducting your system activity reviews, they should understand how critical their roles are for identifying and sounding the alarm against suspicious activities.

If an anomaly is reported, the responsibly for your technical analysis review should fall to your security team, which should work hand-in-hand with your privacy and compliance team to further investigate and evaluate reports.

Remember, these teams should be encouraged to work together; so as you develop your program, be sure to plan, train, and work together as much as possible. Set common goals so you can collaborate and create a better system to protect your ePHI. When working separately, disparate teams often re-invent the wheel and duplicate unnecessary processes. Instead, by creating a system activity review working group that's cross-departmental, you can clearly define responsibilities for each department and integrate those processes between areas of responsibility.

Essentially, no single party should solely be responsible for these reviews. Integrate for success.

Where to begin

So now that you have a better understanding of what a system activity review is and what it's designed to do, how do you get started?

A great starting point is to evaluate and leverage your historical data, for example risk analysis and other assessments such as compliance audits. Once you gather this information, you can identify tasks you're doing correctly (as identified by these audits and assessments). You can adopt these processes as part of your system review without re-inventing processes that already work and are compliant.

When setting up your program, you also don't have to take an all-or-nothing approach. Even at its most basic levels, having something that works for security is better than nothing at all.

Here are a couple of other recommendations as you begin to develop your program:

- **Get leadership support**
  - Demonstrate to your executive team that these reviews aren't just good for business, they're required and failure to do so could cost your company thousands or even millions of dollars. Are they ready to take that risk without it?
- **Create a task force charged with starting your information system activity review program**
  - Gather a dream team to build your program. Include an executive sponsor as well as team members that are actually boots on the ground, using your systems as part of their day-to-day responsibilities.
- **Identify a "get well" date and regularly review your progress**
  - You want to have a pre-determined date that you want to "get well," meaning remediate your gaps and risks, and then plan backward from there based on what you want to accomplish.
- **Don't let these tasks linger.**
  - Remember, they're requirements.

Building your system activity review program

Now, let's take a look at a few simple steps you can implement to build your system activity review program, including processes and policies for success.

1. Know your environment

Begin by conducting a review and develop an inventory of information systems and applications that require system activity reviews. Here's what that might look like:

- Identify systems or applications that create, store, maintain, or transmit ePHI
  - Asset/application/system
  - System administrator/team owner
  - Known SMEs
  - System priority/criticality
  - How many ePHI records
  - Log retention
  - SIEM/FairWarning
  - Log level
  - Review monitoring (manual/automated/hybrid)
  - Frequency of reviews
  - Trigger events
  - Source log location
  - Source log retention
  - Investigative logs (legal hold/security incidents)

- Identify resources and touch points. Know what data your systems record and store.
  - This data may not be limited to your information security team
  - Include privacy/compliance
  - Don't forget your Security Operations Center (SOC)
  - Questions to consider:
    - Which logging capabilities does each system have?

- Are the information system functions adequately used and monitored to promote continual awareness of your system activity reviews?
- Is a policy in place that addresses which reviews you'll conduct and when?
- Are there documented procedures that describe each specific area where you perform reviews?
- Do you conduct reviews reactively or proactively? (You should always be proactive.)

- Map it. Understand your current system activity review lifecycle
  - Include people, processes, and technology
    - Know which reviews are currently in place. Ask information system owners what they do, what works, and what is compliant.
    - Questions to ask:
      - Is there a system activity review already in place? If yes, what does it look like?
      - Have they had any recent events?
      - How did your organization respond to those events?
      - Was it anomalous activity or access?
      - What triggers are used to identify anomalous activity or access?
      - Are these procedures documented?
      - Is the process manual, automated, or is it a hybrid combination of both?
      - How frequently do you conduct reviews?
      - Where's your source log location?
      - What's your source log retention
      - What if you have data that's been pulled out for investigation?

- Leverage the findings as part of your strategic action plan

You want to make sure that you **continuously perform discoveries** within your system for new or adaptive data sources. Over time, you might have systems that change. Your systems are not always static, sometimes they're dynamic.

You also want to make sure that any system that creates receives transmits or maintains ePHI is sending system and application-level logs to your security information and event management (SIEM) tool. Often, this is a manual process, so using a software solution that automates this discovery ensures you've got the data feeds you need going to your SIEM.

2. **Identify and document data generated, recorded, and stored within your system and infrastructure**

This is not an inclusive list, but in general, this step will include discovery of all user login history, failed system access attempts, and ePHI record(s) access, etc.

By discovering and documenting this data, you can get better insight into your data flows. From there, you can analyze data threats (interdependencies and lateral connections) within your environment.

Remember, if you don't know where your data lives, you can't protect it.

3. **Identify and document which systems don't generate actionable logs or reports**

Some of your systems won't generate actionable logs or reports, for example, a legacy system. You can't just ignore these systems because your ePHI can still be at risk. So how do you address systems that do not generate actionable logs or reports? Here are a few tips:

- **Document all systems incapable of producing actionable logs or reports**
  - Before an audit or other assessment (or breach) you'll want to demonstrate you have already identified these issues and you have plans to remediate.
  - Notify security, compliance, and privacy in writing of your findings as soon as discovered.

- **Enforce additional access control measures**
  - For example, can you add multi-factor authentication to it?
  - Can you set a policy where passwords must be changed frequently?
  - Also, consider implementing a Security Operations Center (SOC) or similar team of security staff that can routinely monitor and review all the information that comes through.

- **Increase frequency of user access and permissions reviews**
  - Rather than doing infrequent reviews, such as quarterly or biannually, conduct them more frequently, for example, at least once a month.

- **Implement additional awareness or training specific to the system**

- **Turn off unnecessary or duplicate services, components, protocols, modules, or utilities**
    - If these services are not used, back up the information needed for retention. Securely store that backup and then set the system as read-only.

- **Remove excess, orphaned, or duplicate files and records**

- **Physically or logically isolate these systems**
    - You may want to create a separate segment on your network where you can implement stronger access control lists or other controls. This can help you know what information flows in and outside of these systems.

- **Consolidate or migrate to an alternate product or tool that has actionable logging or reporting capabilities**
    - If you have products in your environment that can be consolidated into one, do so. Consolidate the data and bring it into one system so you have a smaller threat surface to protect.

4. **Prepare information system activity review policies and procedures so they're comprehensive, customized, reasible, agile, and realistic for your environment**

These policies and procedures, which you should view as living, changing, and scalable, are essential in helping your organization identify key roles and responsibilities. It's important you craft these policies and procedures in a language everyone understands.

Also, remember that your policies and procedures should go beyond just system administrator responsibilities. While administrators maintain logs, every employee is a sensor for your organization.

Tips:

- Design and publish a visual aid for the recommended information system activity review process within your organization
- Detail the requirements of what information should be retained within logs and how long it is to reside within the environment

- Document what your organization can and cannot do. You could have limitations that aren't really obvious to an external party, such as OCR, so if you document those limitations and understand them—and you've shown you've tried to mitigate those issues—you may end up with a better outcome than if the auditors or reviewing party discovers the issue for you.

5. Ensure your policies and procedures are actionable

Your system activity review policies and procedures establish a baseline for your centralized security program. These policies and procedures should be clear and actionable and include:

- Roles and responsibilities
- Preparation for conducting system activity reviews
  - Necessary safeguards to protect confidentiality, availability and integrity of audit trails and information system activity review reports
  - Evidence of system activity reviews identifying when, who, and what was reviewed will be retained for a minimum period
  - Automated processes to identify anomalies or unusual activity

- Activity review actions
  - Segregate between system administrators and the system activity review team
  - Build cross-functional, interdepartmental team(s)
  - Remember, when you're developing your other controls, they're not just around system activity reviews but also your termination procedures for departing team members and dissolution of vendor relationships and contracts.

- Follow-up actions
  - Plan for investigation and escalation

6. Educate employees

For program success, ensure all of your employees–regardless of role or department–play an important role in your system activity review lifecycle.

- Employees should understand your comprehensive workforce needs so they also understand consequences of inappropriate action
- Make sure that your all team members are aware that you conduct logging monitoring and that you routinely look at their activity. Be sure everyone understands if they access information outside the scope of their job functions it has repercussions.

7. Continuously review systems, processes, and technology, and develop strategies for improvement and maturity

Earlier, we mentioned you don't have to implement an all-or-nothing approach for your system activity review program. You can develop a program with minimum, compliant standards and then mature your program and processes from there.

- Consider a phased approach that takes into account:
  - The size, complexity, and capabilities of your organization
  - Your technical infrastructure, hardware, and software security capabilities
  - Financial and resource constraints
  - The costs of security measures
  - The probability and criticality of potential risks to ePHI

- Focus on your most critical systems and applications
- Create a roadmap with a defined description of your goals, including steps to reach those goals and assignments for team members
- Set milestones and deadlines
- Routinely evaluate your program's effectiveness and identify gaps
- Create a plan to mature your program over time
- Work with your executive sponsor to communicate your program effectiveness, challenges, and needs to your C-Suite and key stakeholders

Some final tips

A few other tips to help you get started:

- **If your organization has a security information and event management (SIEM) solution:**
  - Perform regular discovery of your environment's systems for new or adaptive data sources
  - Consider implementing a Security Operations Center (SOC) or similar team of security staff that regularly monitor, review, and evaluate technical information

- **If your organization has a patient privacy platform:**
  - Ensure investigators work alongside security staff
  - Have well-defined and progressive sanctions in place, depending on outcome severity

Clearwater is the leading provider of Enterprise Cyber Risk Management and HIPAA compliance software and consulting services for the healthcare industry. Our solutions enable organizations to gain enterprise-wide visibility into cybersecurity risks and more effectively prioritize and manage them, ensuring compliance with industry regulations. Clearwater's suite of IRM|Pro® software products and consulting services help healthcare organizations to avoid preventable breaches, protect patients and their data, and meet OCR's expectations, while optimizing cybersecurity investments. More than 400 healthcare organizations, including 64 of the nation's largest health systems and a large universe of business associates that serve the industry, trust Clearwater to meet their information security needs.

Have questions regarding this white paper? Engage with Clearwater for a specific discussion about your organization's approach.

- ClearwaterSecurity.com/Contact