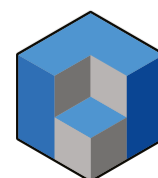


# GET HIP TO HIPAA

## A BEGINNER'S GUIDE TO HIPAA COMPLIANCE

Whether you're just starting out or need a refresher course, this guide from Anderson Technologies covers the most essential aspects of HIPAA and how to achieve compliance.



**ANDERSON  
TECHNOLOGIES**

# CONTENTS

GET HIP TO HIPAA	3
DIVING DEEP INTO THE SECURITY RULE	7
DOCUMENT! DOCUMENT!	17
DOCUMENT!	17
RISKY BUSINESS	23
THE CYCLE OF RISK	33
PLAN FOR THE WORST	40
GETTING STARTED	50
RESOURCES	52
ABOUT ANDERSON TECHNOLOGIES	54

This ebook is intended as a guide to HIPAA and should not be used as your only source of information. All links used throughout this ebook can be found in the Resources section.

# GET HIP TO HIPAA

**E**VEN IF YOU'VE NEVER WORKED IN THE HEALTHCARE INDUSTRY, YOU'VE PROBABLY HEARD OF HIPAA. AN APPOINTMENT TO GET YOUR TEETH CLEANED COMES COMPLETE WITH A SLEW OF FORMS THAT INCLUDE YOUR RIGHTS ACCORDING TO HIPAA. **■** BUT CAN YOU EXPLAIN WHAT HIPAA IS AND WHY THOSE FORMS ARE NECESSARY? WE OFTEN SIGN, DATE AND MOVE ON, KNOWING IT RELATES VAGUELY TO WHAT OUR CARE PROVIDER CAN DO WITH OUR PRIVATE HEALTH INFORMATION.



# HIPAA COMPLIANT

## WHAT DOES HIPAA STAND FOR?

If you're not exceptionally familiar with this acronym, you may think it stands for the Health Information Privacy and Accountability Act. That seems reasonable given how the everyday person is exposed to it. In fact, it stands for the Health Insurance Portability and Accountability Act. That doesn't sound so familiar, does it? In 1996, HIPAA was enacted not with the intent to protect people's privacy, but to regulate and simplify the health insurance industry. According to the [official HIPAA language](#), the objective of this government regulation is:

*"To amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes."*

Essentially, Congress wanted to make health insurance cheaper and simpler by reducing administrative costs and creating a standard method that everyone related to the health insurance industry could adopt. So where does all this privacy and security regulation come into play? The requirement "to simplify the administration of health insurance" triggered everything.

In the Administrative Simplification section of HIPAA, the Act requires that the rights of individuals relating to the use and disclosure of their health information be clearly explained and that standards are set for the electronic exchange of health information. These two subsections, privacy and safeguards, would later be addressed in what are now referred to as the Privacy Rule and the Security Rule.

HIPAA includes a lot more than you may realize, and if you work with Protected Health Information (PHI), especially electronic PHI (ePHI), understanding HIPAA is crucial.



## THE PRIVACY RULE

The Privacy Rule went into effect in 2000 and has been amended several times. It lays out the standards and guidelines for how PHI in all forms—verbal, physical, or electronic—can be used and disclosed. The Privacy Rule is the reason you know the acronym HIPAA at all.

Due to the Privacy Rule, health care providers, insurance companies, and their business partners must follow the same rules regarding health information. Individuals have the same right of access and the same expectation of privacy from all entities according to the guidelines in the Privacy Rule. PHI can include:

- identifiable personal information,
- any medical or mental health condition diagnosed during the lifetime of the individual,
- any treatment or procedure performed in the lifetime of the individual,
- payment information related to healthcare, and
- any identifiable or medical information that the individual wants restricted.

The Privacy Rule is also the reason you must sign that form stating you understand your rights according to HIPAA. Being informed that you have the right to privacy is part of your legal rights. There are exceptions to these rules, such as life-threatening emergencies, court orders, and release of information authorizations, but all are directly addressed and specified within the rule.

Ultimately, the HIPAA Privacy Rule sets the standard for each patient's right to privacy regarding their PHI. Thanks to the Privacy Rule, PHI is automatically considered confidential in almost all circumstances, and it also explains under what circumstances PHI may be shared.



# THE PRIVACY AND SECURITY RULES


## THE SECURITY RULE

The Security Rule is a little different. It first went into effect in 2003 and, unlike the Privacy Rule, relates only to ePHI. The Security Rule established the safeguard standards everyone dealing with ePHI must follow to be HIPAA compliant. Compliance means all ePHI is stored, processed, and transferred in a way that ensures patient privacy. While it doesn't dictate specific implementation steps, since each company's use and needs around ePHI is different, anyone dealing with ePHI must address each specification.

HIPAA began as a way to simplify health insurance procedures and make those handling health information more accountable to every citizen's rights about their private health information, and its effects have been far-reaching. For anyone dealing with PHI, the requirements can appear daunting at first, but with a trusted IT partner, HIPAA compliance means any and all health information will be safe in your hands.

# DIVING DEEP INTO THE SECURITY RULE

HIPAA's Security Rule may seem daunting at first, especially if you're not an IT expert, but you don't need a degree in computer science to understand the standards it establishes.



AT ITS CORE, THE HIPAA SECURITY RULE IS ABOUT KNOWING WHAT DATA YOU HAVE, ASSESSING THE PEOPLE AND TECHNOLOGY HANDLING IT, AND FINDING WHERE PROBLEMS COULD ARISE. SURVEY, ASSESS, PLAN, IMPLEMENT, AND—MOST IMPORTANTLY—REPEAT. THIS IS AN EASY WAY TO THINK ABOUT AND MANAGE THE REQUIREMENTS LAID OUT IN THE SECURITY RULE.



## WHAT EXACTLY DO CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY MEAN TO EPHI?



### CONFIDENTIALITY

Don't allow anyone without proper permission to access ePHI, as described in the Privacy Rule, to see it.



### INTEGRITY

Ensure that the ePHI created, maintained, or transmitted isn't altered in any way.



### AVAILABILITY

Ensure those with permission are able to access ePHI when they need it.

## WHAT IS THE SECURITY RULE?

**The Security Rule** sets the standards that entities creating, using, or transmitting electronic protected health information (ePHI) must implement in order to “ensure the confidentiality, integrity, and availability of ePHI . . . protect against any reasonably anticipated threats and hazards... [and] protect against reasonably anticipated uses or disclosures of such information not permitted by the Privacy Rule” ([NIST](#)). If you can imagine it happening to you, then you have to protect against it. ■■■■■

### CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY

The Security Rule uses this phrase throughout. It's a key tenet of its purpose, but what exactly does it mean to ePHI? Confidentiality, integrity, and availability aim to ensure that ePHI remains private, unaltered by accidental or malicious means, and is ready when needed. A quick way to think of these is “Don't Show. Don't Change. Can Use.” Keep these goals in mind when implementing the standards set forth in the Security Rule.

# UNDERSTANDING THE SECURITY STANDARDS

THE SECURITY RULE IS DIVIDED INTO THREE SECTIONS: ADMINISTRATIVE, PHYSICAL, AND TECHNICAL.

The Security Rule consists of 18 security standards divided into three sections: Administrative Safeguards, Physical Safeguards, and Technical Safeguards. Some of those security standards contain implementation specifications (36 total), which provide more detailed instructions on what needs to happen to fulfill the security standard. The Security Rule designates these implementation specifications as either required or addressable.

Do not confuse addressable with optional. All implementation specifications must be handled, but those marked as addressable may not be suitable for all businesses managing ePHI. Each business must assess its own situation to determine whether an addressable implementation specification is reasonable and appropriate. Once assessed, the business has to ask:

Each business must assess its own situation to determine whether an addressable implementation specification is reasonable and appropriate. Once assessed, the business has to ask:

## REASONABLE AND APPROPRIATE

The Security Rule was designed with flexibility of approach in mind. Many of its standards explain **what** needs to be done, but leaves **how** to implement them up to the individual business, based on its use of ePHI and its environment. According to general rule §164.306(b) (2), covered entities and business associates must take into account the following factors:

### 1

The size, complexity, and capabilities of the covered entity or business associate.

### 2

The covered entity's technical infrastructure, hardware, and software security capabilities.

### 3

The costs of implementing the security measures.

### 4

The probability and criticality of potential risks to ePHI.

## IMPORTANT!

DO NOT CONFUSE ADDRESSABLE WITH OPTIONAL.

ALL ASSESSMENTS AND JUSTIFICATIONS FOR NOT IMPLEMENTING A SPECIFICATION AS STATED IN THE SECURITY STANDARD MUST BE FULLY DOCUMENTED.

- ▶ **Is the specification reasonable and appropriate?**  
Yes—Implement.
- ▶ **Is the specification not reasonable or appropriate?**  
No—Implement an alternate solution that would be.
- ▶ **Are there any reasonable and appropriate ways to implement the specification?**  
No—Do not implement.

Flexibility, scalability, and technology neutrality are key features of the Security Rule that allow businesses of any size or function to use the same standards and adjust accordingly to the evolution of technology. It's important to note that cost alone does not justify refusal to implement a security standard. All factors need to be considered together when dealing with addressable specifications.



## SECURITY STANDARDS

Before diving into the nitty-gritty of each security standard and the implementation specifications, evaluate what your business already has in place. Some of the requirements may be satisfied by your current security infrastructure.

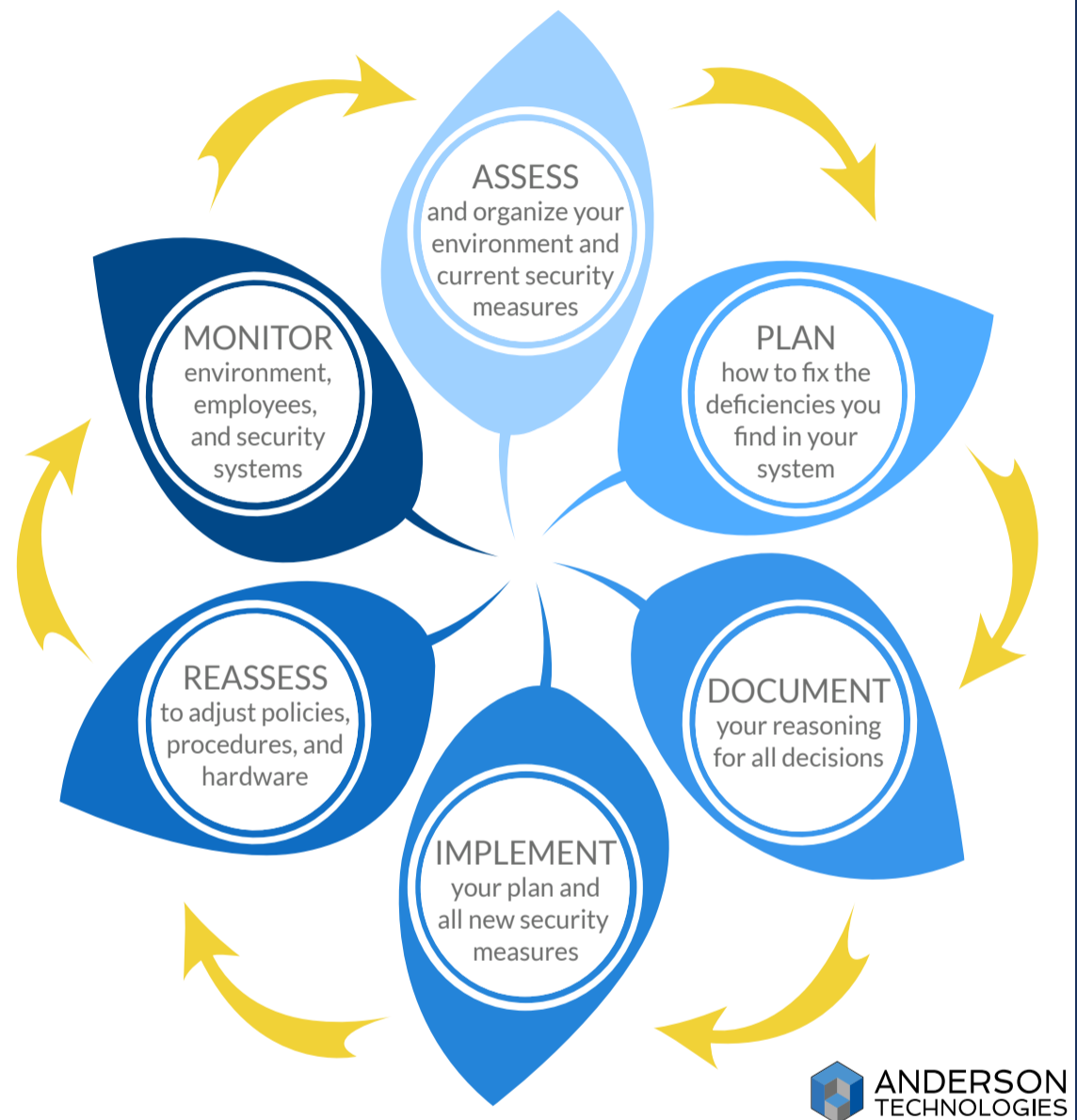
Read all the security standards once to get a feel for what you need to be assessing, then take the time to determine what measures, policies, and hardware already protect your ePHI. Knowing where you stand can save you time and stress while working toward HIPAA compliance.

The following will address each section in a high-level overview and mention important standards you should be aware of. This won't be a step-by-step breakdown of all the standards and implementation specifications. For that, the [Department of Health and Human Services](#) (HHS) produced the HIPAA Security Series papers, which are extremely helpful, as is National Institute of Standards and Technology's (NIST) [An Introductory Resource Guide for Implementing the HIPAA Security Rule](#).

# ADMINISTRATIVE SAFEGUARDS

**Administrative Safeguards** make up more than half of all the standards in the Security Rule; however, this is also where many of your current systems might already be established and satisfy the requirements with little to no alterations. The standards and implementations categorized under Administrative Safeguards involve the process of planning, selecting, and managing a business's protection of ePHI. This includes, but is not limited to, emergency preparedness plans, policies and procedures, contracts, and employee management and training. This category is all about knowing what you have, planning for the future, and making sure everyone in the organization knows how to enforce the confidentiality, integrity, and availability of ePHI. Simply implementing these systems is not enough, though. Everything must be documented, accessible to all who need it, tested, and reviewed periodically.

## THE RISK ANALYSIS AND MANAGEMENT PROCESS



## SECURITY MANAGEMENT PROCESS

### §164.308(A)(1)

This is the very first standard, and for good reason. Its implementation specifications require a risk analysis and continuous risk management. The information gathered in these steps will help with many of the other standards. The risk analysis can highlight areas of deficiency in your security that might otherwise appear only when a malicious actor finds and exploits it.

There is no single correct way to perform a risk analysis because all businesses have differing needs. If you are looking for where to start, there are many useful guides outlining the risk assessment process. The HHS's HIPAA Series includes Basics of Risk Analysis and Risk Management, and Appendix E in NIST's Introduction provides risk assessment guidelines. For a more comprehensive look at risk assessments, NIST also produced a Guide for Conducting Risk Assessments.



## WORKFORCE SECURITY

### §164.308(A)(3) &

### SECURITY AWARENESS AND

### TRAINING §164.308(A)(5)

These two standards have seven addressable implementation specifications between them. These deal with verifying that employees have the correct access to ePHI according to the duties they perform, and that they are informed on how to protect themselves and ePHI from cybersecurity threats. These also deal with how management handles adding new employees and removing employee access as job duties change or if an employee leaves the company. Both management *and* employees are responsible for protecting ePHI and must be given the knowledge, tools, and policies to do so. ■■■■■

## CONTINGENCY PLAN

### §164.308(A)(7)

This standard includes the creation of several different emergency preparedness plans, including a Data Backup Plan, Disaster Recovery Plan, and Emergency Mode Operation Plan. Besides guiding both management and employees in what to do, who needs to do it, and where resources are during an emergency, this standard also helps assess what hardware or software is critical to the confidentiality, integrity, and availability of ePHI. This assessment allows better prioritization and distribution of limited resources. Such precise knowledge is especially important for facilities that provide direct patient care. ■■■■■

---

# DOCUMENT

---

# EVALUATE

---

# TEST

---

# MONITOR





## DEVICE AND MEDIA CONTROLS §164.310(D)(1)

Given the portability of data in the daily functions of modern business, any movable media containing ePHI must be strictly logged, tracked, and disposed of when no longer needed. Even one lost USB drive containing ePHI is a breach of the Security Rule. This standard relates to all types of removable media, including laptops, flash drives, CD/DVDs, hard drives, and portable backups. It also deals with the re-use of these materials within the office, which first requires the proper removal and destruction of all ePHI.

## PHYSICAL SAFEGUARDS

Physical Safeguards deal with the facility, hardware, and other physical mechanisms necessary to protect ePHI, as well as the policies and procedures that regulate them. These can range from locks on doors or security guards in times of disaster to employees logging off before leaving a workstation. If a person could walk into your office and potentially access ePHI, the Physical Safeguards handle how to appropriately plan your security measures according to your needs.

For the Security Rule, physical safeguards refer only to ePHI storage and use, but the storage and care of paper PHI can easily fit into an audit of physical safeguards.

# TECHNICAL SAFEGUARDS

Technical Safeguards deal with the technology used to create, access, transmit, and protect ePHI, as well as the policies and procedures that govern it. The Security Rule remains intentionally vague on the specific technology used to fulfill these standards to allow for advances in technology and the changes in security needs against new cybersecurity threats. This flexibility is also what allows a variety of businesses to handle ePHI and still comply with HIPAA's Security Rule. ■■■■■



Technical Safeguards address aspects such as user access, hardware and software use, transmitting ePHI digitally, and encryption for various purposes. The Risk Analysis and Risk Management specifications from Administration Safeguards are especially useful in determining the technological needs and policies to enforce.

## INTEGRITY §164.312(c)(1)

This standard refers directly back to the key phrase confidentiality, integrity, and availability discussed earlier in this ebook. Merely protecting ePHI from being accessed or transmitted improperly is not enough to ensure its integrity. All ePHI must also be protected from tampering or destruction of data. Wrong or incomplete information can have drastic effects on patient lives and care, so the ability to authenticate the validity of ePHI is an essential element of its security.

## MONITOR AND UPDATE

Assessing and creating policies aren't the only essential parts of the Security Rule. Implementing those policies so all employees are aware of and following the rules cannot be overlooked. Systems should be in place to verify that employees receive the necessary training in ePHI security procedures and understand the consequences of not following the policy. Reassessment of policies and retraining of employees should occur periodically so outdated procedures can be rewritten for the current threat environment. As [cyber threats are ever evolving](#), so too should ePHI cyber protections.

While the Security Rule may feel a bit daunting, many of its requirements are best practices for any business. Knowing exactly what data you handle, how it's processed, and who needs to access it provides you with an informed view of your business's operations. Having a written and tested [Disaster Recovery Policy](#), Contingency Policy, and Continuity of Operations Plan will save you time, money, and stress should an emergency occur.

# 8.5M

INDIVIDUALS AFFECTED IN BREACHES  
IN 2018 AS REPORTED ON THE  
[HSS WALL OF SHAME](#)

# 61%

OF ALL HHS INVESTIGATIONS IN 2018 REQUIRED CORRECTIVE ACTION BY THE COVERED ENTITY OR BUSINESS ASSOCIATE UNDER REVIEW. ([ENFORCEMENT RESULTS BY YEAR](#))

TOP 5 ISSUES REQUIRING  
CORRECTIVE ACTION IN 2018\*

- 1 IMPERMISSIBLE USES & DISCLOSURES
- 2 SAFEGUARDS
- 3 ADMINISTRATIVE SAFEGUARDS
- 4 ACCESS
- 5 TECHNICAL SAFEGUARDS

\*([HHS DATA BY YEAR](#))



DOCUMENT!  
DOCUMENT!  
DOCUMENT!

**N**EARLY ALL THE IMPLEMENTATION SPECIFICATIONS REQUIRE SOME FORM OF POLICY AND PROCEDURE DOCUMENTATION. THIS INVOLVES MORE THAN THE REASONING AND JUSTIFICATION FOR HOW YOU CHOOSE TO IMPLEMENT THE SPECIFICATIONS (THOUGH THAT MUST BE DOCUMENTED AS WELL). THESE ARE THE POLICIES AND PROCEDURES THAT HIPAA EXPECTS YOUR BUSINESS TO FOLLOW EVERY DAY.



# ORGANIZATIONAL STANDARDS

IF YOU WORK WITH OR ARE A BUSINESS ASSOCIATE WHO WORKS WITH EPHI AND YOUR CONTRACT HAS NOT BEEN UPDATED SINCE THE [HITECH ACT](#) IN 2009 OR THE [FINAL OMNIBUS HIPAA RULE](#) IN 2013, YOU WILL WANT TO REVIEW AND UPDATE ALL CONTRACTS TO ENSURE THEY MEET THE CURRENT STANDARDS REGARDING BUSINESS ASSOCIATES.

Besides the administrative, physical, and technical safeguards which make up the majority of the Security Rule, there is a lesser known section of safeguards called organizational standards that deal largely with the paperwork required by HIPAA concerning protected health information (PHI) in any form. This section is often overlooked because many of its requirements are addressed in greater detail throughout the Privacy and Security Rules. The four standards in this section include:

- [Business Associate Contracts](#)
- [Requirements for Group Health Plans](#)
- [Policies and Procedures](#)
- [Documentation](#)

This section focuses on the last two standards: Policies and Procedures and Documentation, both of which lay the groundwork for HIPAA compliance. The other two standards shouldn't be ignored, but they concern only those who (1) are or need a business associate or (2) are a sponsor to a group health plan that provides data beyond enrollment and summary information.

## POLICIES AND PROCEDURES §164.316(A)

Why have an entire standard dedicated to something addressed in nearly every single implementation standard? This standard explains what HIPAA expects from the policies and procedures that a business creates. Specifically, it references the Security Standards' General Rule of Flexibility of Approach. It also allows for policies and procedures to be changed at any time to adjust to new demands or technologies as long as all changes are documented and implemented accordingly.

## DOCUMENTATION §164.316(B)(1)

This standard identifies how documentation required by HIPAA is to be maintained. According to this standard and its subsequent implementation standards, all documentation required throughout the Security Rule's standards, including but not limited to

- [policies and procedures,](#)
- [job responsibilities and duties,](#)
- [risk assessments, and](#)
- [action plans,](#)

must be recorded (physically or electronically) and retained for a minimum of six years from the date of creation or when it was last in use, whichever date is later. All documentation must be available to anyone who uses those procedures, and documentation should be consistently reviewed and updated as necessary.

THE SIX-YEAR RETENTION RULE ONLY SATISFIES HIPAA STANDARDS. STATE LAW MAY REQUIRE SOME DOCUMENTATION TO BE RETAINED FOR LONGER. ALWAYS VERIFY WHAT STATE LAWS APPLY TO YOUR BUSINESS AS HIPAA DOES NOT SUPERSEDE MANY STATE REQUIREMENTS.

It's possible your business already has clear policies and procedures in place, but that doesn't immediately make you HIPAA compliant. You still need to go through each one to ensure it satisfies the implementation specifications it pertains to. If not, policies may need to be updated or new ones added. HIPAA gives businesses a great deal of leeway in how policies and procedures are written, so both updating existing documentation and creating all new materials is acceptable.

### WHAT SHOULD THE POLICIES AND PROCEDURES SAY?

HIPAA doesn't dictate the exact wording of any policy or procedure. It's up to the business, taking into consideration the Flexibility of Approach guidelines, to determine what policy needs to be implemented. Generally, a policy explains a business's approach to the subject it relates to. If the policy concerns removing access from those who no longer work for the company, it could read something like:

At the end of an employee's last day of employment with [company name], security and/or IT staff will remove that employee's access to company systems and restricted locations and document the change of access. The employee's supervisor will verify that all access has been revoked within twenty-four hours.



## BRINGING YOUR POLICIES INTO COMPLIANCE

This offers clear guidance about what the company intends to do to remove access from someone who no longer is allowed to work with PHI. It also dictates an implementation timeline, who should implement the policy, and how the company will ensure it gets implemented properly.

The procedure that accompanies the policy would then offer easy-to-follow directions on how those responsible are to implement the policy. A sample procedure may look like the example below.

### REGARDING POLICY FOR REMOVING ACCESS OF FORMER EMPLOYEES: DUTY OF IT STAFF OR MANAGED SERVICES PROVIDER

1. Go to [directory] and locate the list of all programs and devices employee had access to according to job title. Check this list against their user account to ensure no programs are missed.
2. Starting at the top of the list, go through each program and device and remove employee access. For procedures regarding specific programs, see [directory of procedures].
3. Go to Active Directory and find employee information.
4. Backup emails and save them to [directory] to be stored for a period of one year before deletion.
5. Backup any information relating to patient care in appropriate directories. See [directory list] for proper placement.
6. Disable user's Active Directory account and change their password.
7. Document time, date, and your name in the Employee Termination log to indicate all access has been removed.
8. Inform former employee's supervisor when access removal is completed for them to verify.

Procedures should be as detailed as possible so that there is no ambiguity or confusion in what needs to be done. This allows newer employees to accomplish tasks they may not have performed before. There may also be multiple procedures related to the same policy depending on the duties of each person. Margaret Amatayakul wrote an excellent [guide to creating policies and procedures](#) for the Journal of AHIMA (American Health Information Management Association).

## NOTE

Both the Security Rule and the Privacy Rule require policies and procedures to be created. A company can combine relevant Security and Privacy standards into a single policy or create entirely separate policies for the Security and Privacy Rules. Each business should determine what is best for its employees.



# EMPLOYEE TRAINING

Once you have your policies and procedures written and accessible, the next big step is to train employees on them. HIPAA requires all employees to be trained in the policies and procedures related to their job. Training should include everyone from the maintenance staff to the CEO. Each time a policy or procedure is updated, retired, or replaced, the affected staff must be informed and, if needed, new training should occur.

Of course, maintenance personnel and CEOs won't need the same kind of HIPAA training, just as IT support personnel doesn't need the same training as a nurse. HIPAA doesn't dictate the way training happens, only that it happens. This means big companies that can afford professional training materials may use them, while smaller companies might only hold informational meetings. Each company can train in most effective way for them.

## SUGGESTIONS FOR EMPLOYEE TRAINING

- Go through your employees' job descriptions and separate employees by the level of access they have to PHI.
- Create training programs for each level of access and/or the duties required in the job description so each employee gets the training suited to their job.
- Don't overload employees with policies and procedures that don't relate to their jobs.
- Ensure all training includes how to access the company's policies and procedures in case employees need to revisit or reference them.
- Ensure that all employees know who to contact if they have questions.





## SANCTIONS

ALONG WITH EMPLOYEE TRAINING, HIPAA ALSO REQUIRES YOU HAVE CLEAR CONSEQUENCES FOR NOT FOLLOWING THE WRITTEN POLICIES AND PROCEDURES. THE TYPES OF OFFENSES SHOULD BE CLEARLY DEFINED AND THE DISCIPLINARY ACTION ENACTED FOR EVERY INFRACTION.

One way a company might dictate levels of disciplinary action would be to clarify whether a break in policy or HIPAA standard was accidental, made through negligence, or if it was of malicious intent. This allows various consequences for the same infraction without being inconsistent. Examples would be:

- a) [an employee leaving a workstation unlocked because an emergency situation demanded they respond immediately,](#)
- b) [they consistently forget to lock their workstation even after being warned about it, or](#)
- c) [they intentionally leave a workstation unlocked to allow someone without access to view ePHI.](#)


While the infraction is technically the same, the situations don't deserve the same consequences. As with everything else, all infractions and disciplinary actions need to be documented and retained for six years.

In 2019, the Health and Human Services' Office of Civil Rights reported [430 breaches of PHI](#), each resulting in at least 500 individuals affected, though often that number was much higher. Policies and procedures may feel tedious to write, but they provide employees with all the information necessary to do their jobs in a HIPAA compliant manner and could prevent a breach of PHI.

# RISKY BUSINESS



No matter the size of your practice, compliance with the HIPAA Security Rule is a serious undertaking. In order to fix a problem, you must first know it exists. That's why the Risk Analysis and Risk Management implementation specifications are the foundation of your security compliance efforts.



THE IMPORTANCE OF PERFORMING A THOROUGH RISK ANALYSIS AND COMING UP WITH A RISK MANAGEMENT STRATEGY CANNOT BE OVERSTATED. THROUGHOUT THIS SECTION THERE WILL BE LINKS TO RESOURCES TO HELP YOU DECIDE HOW BEST TO PERFORM YOUR RISK ANALYSIS. IF YOU'VE NEVER PERFORMED A RISK ANALYSIS, WE STRONGLY SUGGEST GOING OVER THOSE RESOURCES FIRST.



# WHAT IS A SECURITY RISK ANALYSIS?

While much of this section presents an outline of how to conduct a Security Risk Analysis (SRA), it first helps to understand what an SRA is. Identifying that a problem exists—or could exist—is crucial to fixing it, preventing it, or making it as safe as possible.

An SRA is ultimately a process that allows you to analyze the way your company approaches risk and see how all areas of your business or organization—from policies and procedures to technical implementation—influence each other. It creates lists of threats, vulnerabilities, and threat events which could impact not only your organization, but your patients, customers, or vendors as well. Once you understand the risk in your daily business functions, finding a solution to keep them secure and operational is much easier.

The SRA process is complicated and can require a substantial investment of time and effort to complete, depending on the size and scope of your business. But when it's finished, the SRA will provide you with a blueprint for the future. It identifies areas that are protected, areas that could use some fixing, and areas that are desperately unprotected. This allows you to prioritize your needs and create a risk management strategy specific to your environment. When going through your HIPAA Security Rule compliance, there's no better tool than an SRA.

## THREAT

The potential for a person or thing to trigger or exploit a vulnerability.

## VULNERABILITY

A flaw or weakness in the system security procedures, design, implementation, or internal controls that could be accidentally triggered or intentionally exploited and result in a security breach or a violation of the system's security policy.

## THREAT EVENT

How a particular threat could trigger or exploit a specific vulnerability thing to trigger or exploit a vulnerability.

([NIST 800-30](#))



An SRA can feel overwhelming. Don't think you have to go it alone, though. Anderson Technologies has partnered with industry experts to help make the compliance process less daunting.

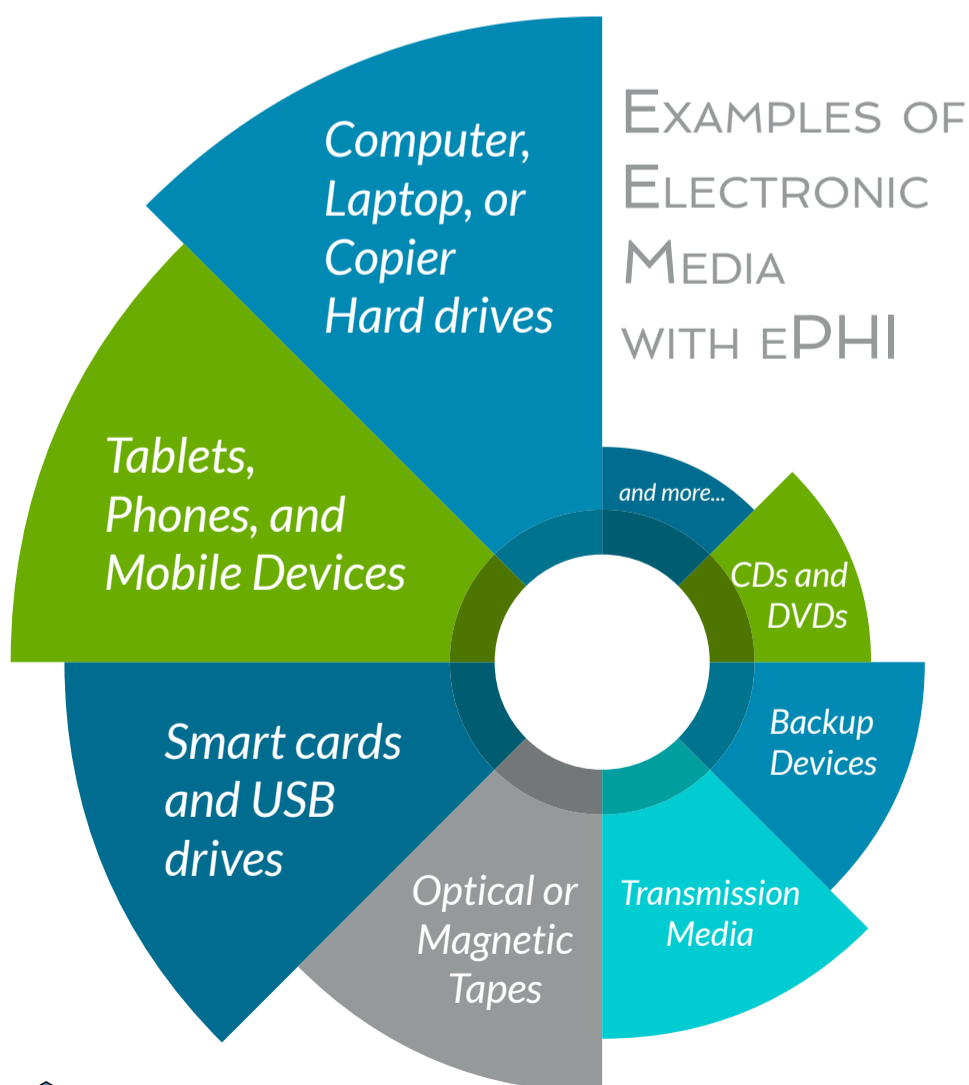
# WHY DO YOU NEED AN SRA?

For HIPAA, you must conduct a targeted SRA. §164.308(a)(1)(ii)(A) requires an “accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information. . . .” The key to this is the specification of electronic protected health information (ePHI).

Since the Security Rule only deals with ePHI (where the Privacy Rule handles all PHI), the SRA only needs to focus on the ways in which ePHI is created, received, maintained, or transmitted. Including or performing a second SRA to include all PHI and the ways it could be improperly handled or disclosed would be best practice to assess your policies and procedures regarding non-electronic PHI, but it’s not required

under HIPAA. It’s important to remember that ePHI involves far more than an electronic health or medical record system. It includes all types of electronic media hardware that can create, receive, maintain, or transfer ePHI, as well as software such as appointment calendars or billing databases.

While it can only help your organization to conduct a business-wide risk analysis, the targeted scope of ePHI under HIPAA narrows what you need to assess. Don’t narrow your field too much, though. The cost of insufficient or non-existent SRAs and risk management plans can lead to data breaches and serious fines.



According to the Office of the National Coordinator (ONC) for Health Information Technology, simply filling out a checklist is not enough to complete an SRA or count as proper documentation under HIPAA. You can learn more about common misconceptions about the SRA at the [ONC’s website](#).

# PREPARING FOR AN SRA

## GUIDES AND TOOLS TO HELP YOU CONDUCT AN SRA ON YOUR OWN

While no tool can replace a thorough and accurate SRA, there are plenty to assist you during the process. The ONC has an [SRA Tool](#) that you can download to help identify areas that may need improvement. They also have [video tutorials](#) and [interactive games](#) to test your knowledge of both privacy and security requirements.

There are also numerous guides to help you better understand the process of risk analysis and management. Besides what we've mentioned in previous sections (the Department of Health and Human Services' (HHS) [HIPAA Security Series](#), and [NIST's Introductory Resource Guide—Appendix E](#), both [the ONC](#) and [the HHS](#) have overviews of the risk analysis process.

For detailed explanations of the risk analysis and management process, NIST published two separate guides: [SP 800-39 Managing Information Security Risk](#) and [SP 800-30 Guide for Conducting Risk Assessments](#). These are not specifically geared to HIPAA's SRA, but the level of information provided is far more complete than many of the HIPAA-specific



guides. We recommend that you read SP 800-39 before SP 800-30. While SP 800-30 offers greater detail about specific parts of the risk analysis process (especially in the appendices), SP 800-39 is more reader friendly and a good foundation for SP 800-30.

### CHOOSING AN OUTSIDE CONTRACTOR

If you do not feel confident enough to perform an accurate and thorough SRA even with these tools, or simply do not have the time to research and learn enough to perform an accurate and thorough SRA, outside contractors and software solutions can help. Be careful when vetting an auditor or software offering SRA capabilities. Make sure they have a proven history of clients successfully passing audits because of the SRA they performed. An incomplete SRA can cost your business just as much as no SRA.

**A COMPLETE LIST OF  
RECOUCES IS PROVIDED  
AT THE END OF THIS  
EBOOK.**





# How to Conduct an SRA

WHILE GOING THROUGH THE STEPS, IT'S IMPORTANT TO REMEMBER TO LOOK AT RISK FROM AN **ORGANIZATIONAL** PERSPECTIVE (BUSINESS-WIDE POLICIES AND PROCEDURES OR BUDGETS), A **BUSINESS FUNCTION** PERSPECTIVE (BILLING OR PATIENT CARE), AND AN **INFORMATIONAL SYSTEMS** PERSPECTIVE (SETTINGS ON SPECIFIC TECHNOLOGY OR HARDWARE PURCHASES). ANOTHER WAY TO LOOK AT THIS WOULD BE **ADMINISTRATIVE, PHYSICAL, AND TECHNICAL** LENSES TO MATCH UP WITH THE HIPAA SAFEGUARDS. IF YOU PREFER HIPAA TERMINOLOGY, KEEP IN MIND THAT PHYSICAL ISN'T PERFECTLY ANALOGOUS TO BUSINESS FUNCTION.

## SCALABILITY AND FLEXIBILITY ARE AT THE CORE OF THE SRA.

A two-dentist practice isn't going to need the same kind of SRA as a large nursing facility, so HIPAA doesn't dictate the exact steps to conducting an SRA. However, all thorough and accurate SRAs will go through similar steps and feature key information, no matter the format you choose. As always for HIPAA, document each step for the final SRA report.

### 1 GATHER INFORMATION

An SRA shouldn't be performed by one person. Business owners or senior leadership should work together with management and IT experts during the SRA process. Not everyone sees risk the same way, and having a knowledgeable team ensures that your SRA will identify risk from all necessary perspectives. ►

No matter the size of your business, compliance with the HIPAA Security Rule is a serious undertaking.

## 2 DETERMINE THE SCOPE

In this case, HIPAA has defined the scope for you in §164.308(a)(1)(ii)(A): “the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information” wherever it is created, received, maintained, or transmitted.

If it holds, accesses, or transmits ePHI, it needs to be part of the SRA. For some businesses this will be a lot to cover, while others may only reference a few systems. Though the scope may be increased to include both physical and electronic PHI, it should never be reduced.

## 3 CREATE A RISK ANALYSIS FRAMEWORK

A risk analysis framework isn't required for an SRA, but it's a useful tool to maintain consistency and avoid ambiguity between those preparing the SRA, those implementing it, and those conducting future SRAs. Since few people see risk the same way, the framework creates a clear set of assumptions, constraints, risk tolerances, and priorities/tradeoffs that will determine how your business manages risk.

Many of these terms appear in later steps, but they're not used in the same way. In the framework you explain how to identify and respond to the risk factors, while later you use the framework to actually identify and respond to the risk. The framework puts everyone on the same page so that each person knows what to look for, how to judge the risk, and how to manage that risk appropriately.



The framework should also dictate the methodology you use to conduct this and future SRAs. This can be qualitative (high, medium, low), quantitative (numerical quantities), or a mix of both. Not all risk can be numerically quantified (number of individuals affected vs. lost reputation), so a qualitative or mixed approach can be more useful.

If you choose to skip the framework step, much of this information will still need to be explained in later steps to satisfy documentation requirements, and you won't have it available for subsequent SRAs. ►

### RISK ASSUMPTIONS

Identify how risk is assessed, responded to, and monitored in your business.

Assessment methodology should be defined in this step.

### THREAT SOURCES

Make explicit the types of threats to be considered (and any assumptions about them) and provide examples.

Determine credible sources to be used to identify threats.

### RISK TOLERANCE

Determine how much risk you are willing to accept while remaining HIPAA compliant.

A company with high risk tolerance will accept more risk than one with a low risk tolerance.

### PRIORITIES & TRADE-OFFS

Decide what is addressed first and with what resources.

All risk must be addressed, but some fixes are more vital. Focus on creating an effective plan for allocating resources over time.

## 4 GATHER DATA

In order to determine the risk to ePHI, you must first determine where it is stored, received, maintained, and transmitted. And while this encompasses a great deal more than physical hardware, having a record of the physical hardware and its movements is a part of Physical Safeguards (§164.310(d)(2)(iii)—Accountability). This is especially important as more and more healthcare settings utilize portable electronic media, such as tablets or laptops.

Think of the flow of ePHI. Where does it begin in your business? Do you create it or receive it? Follow it from its starting point to endpoint and document what systems each piece of ePHI interacts with. Depending on your business, this could be only a few pieces of software and hardware or it could be most systems in the office. Either way, you need a complete list in order to conduct a HIPAA-compliant SRA.

## 5 IDENTIFY AND DOCUMENT POTENTIAL THREATS AND VULNERABILITIES

This could be considered one step or two, depending on how you decide to conduct your SRA. It may be simpler to identify potential threats and vulnerabilities separately, but you may find that as you identify a threat, you also identify the vulnerability it could exploit and vice versa. It is up to your team to decide the best method.

If you've already created a framework, you're ready to identify threats and vulnerabilities. If not, take some time to decide what you're going to consider a threat or vulnerability, how you'll identify them, and what sources are valuable to work from during the process.

Sources of information could include past SRAs, business security reports or testing,

known breaches of similar institutions ([Breach Level Index](#), [OCR Breach Report](#)), the security community's public lists and advisories ([National Vulnerability Database](#), [National Checklist Repository](#)), information from vendors, and your managed services provider or IT staff.

### THREATS

One important thing to note when starting your list of potential threats is that you are not required to list **all** potential threats. You must list **all reasonably anticipated threats** to ePHI. Having valuable sources of threat information is important because you don't want to waste time or resources on a threat that will never affect you, such as a hurricane if you're nowhere near the ocean.

At this point you're not looking at whether or not you've already mitigated the risk of such threats affecting ePHI. You're only considering whether it is a reasonably anticipated threat. Threats aren't just about whether someone steals your data for misuse, but whether you can verify the integrity of your ePHI and have it available when you need it. ▶

REMEMBER TO DOCUMENT EVERYTHING THROUGHOUT THE SRA PROCESS.





## VULNERABILITIES

When dealing with ePHI, it's easy to think of vulnerabilities as technical problems. Non-technical vulnerabilities cannot be overlooked and can even be the root problem to other perceived vulnerabilities. Misconfiguration of security settings or poor hardware purchasing could lead to a number of technical vulnerabilities. This can happen due to a lack of policies and procedures on setting up new hardware or a budget that doesn't meet the demand of current threats. This is why a team is important for looking at both the big picture and the small details.

## 6 ASSESSING SECURITY MEASURES

Now that you have a complete list of threats and vulnerabilities, it's time to see what security measures you already have in place to protect ePHI. Small- to medium-sized business have a greater degree of control over their environment, which is an advantage in mitigating risk. Like vulnerabilities, security measures can be both technical and non-technical and should be looked at from all perspectives. When documenting, also record that all technical security measures are not only there but also configured and utilized correctly.

## 7 DETERMINING RISK

In order to determine risk, it's time to put the threats and vulnerabilities together to create a list of possible threat events. This is not a strictly one-to-one pairing. A single threat might affect multiple vulnerabilities, and a single vulnerability might be affected by multiple threats. (For more guidance on threat events, see [Appendix E of SP 800-30.](#))

For each threat event, you must determine the likelihood of it occurring and the impact it would have on ePHI and your business if it did. Likelihood is the probability that a threat event will occur.

Below are examples (both qualitative and quantitative) of how you could determine likelihood and impact. Depending on your business's risk tolerance, you might add more levels beyond high, medium, and low.

QUALITATIVE	QUANTITATIVE	DEFINITION OF LIKELIHOOD
HIGH	67 - 100	Threat event will definitely occur or has a high probability of occurring. Insufficient safeguards, uncontrollable environmental factors, or poor policies and procedures could all contribute.
MEDIUM	34 - 66	Threat event has a moderate possibility of occurring. Safeguards are in place but poorly configured or employees are not trained on policies to mitigate risk could contribute.
LOW	1 - 33	Threat event is not likely to occur. Safety measures are properly implemented to counter the threat.

The impact of a threat event can be felt across different levels. The most obvious is the direct breach to ePHI's confidentiality, integrity, and availability, but impact can also be felt in the loss of revenue from a damaged reputation, the cost of fixing the effects of the threat event, time and effort spent dealing with regulatory audits, and other intangible results. Below is an example of how you might measure impact. ►

QUALITATIVE	QUANTITATIVE	DEFINITION OF IMPACT
HIGH	67 - 100	Threat event could have severe or catastrophic effects on ePHI and/or the business. This could be measured by number of people affected or the type of ePHI breached.
MEDIUM	34 - 66	Threat event could have serious effects on ePHI and/or the business.
LOW	1 - 33	Threat event could have a limited effect on ePHI and/or the business.





### LEVEL OF RISK

Accurate assessments of the above are vital to determine the overall level of risk posed by a threat event, because risk is a combination of likelihood and impact. For example, if the impact is high but the likelihood is low, then the overall risk would be low. The clearer the definitions in the framework of what constitutes the levels of likelihood and impact, the more accurate and consistent your evaluations of threat will be. Threat matrices (such as those in [Appendix I of SP 800-30](#)) can be used for both qualitative and quantitative methodologies.

## 8 DOCUMENT AND MANAGE RISK

If you've kept up with your documentation, the final SRA report should be simple to put together. [Appendix K of SP 800-30](#) offers a base template for writing an SRA report, but you should tailor it to your business' needs. In general, it should include all the lists you've made, as well as the reasons for your determinations and how you plan to use this information.

The final task of an SRA is to develop a risk management plan. HIPAA understands that risk cannot be wholly eliminated, but it should be reduced to reasonable and acceptable levels. Conducting an SRA and implementing a risk management plan become the foundation for implementing the rest of the Security Rule's safeguards. In the next section, we'll look at how to use your SRA to create a risk management plan.

## HITECH

In 2009, Congress passed the HITECH Act. Among other changes, the HITECH Act made business associates directly liable under HIPAA and required them to be held to the same security and privacy standards as covered entities.


# THE CYCLE OF RISK



THE SRA SERVES AS A STARTING POINT FOR FULFILLING MANY OF THE STANDARDS OF THE SECURITY RULE, BUT ITS MOST IMPORTANT FUNCTION IS TO HELP YOU CREATE A RISK MANAGEMENT PLAN TO MITIGATE AND MONITOR THE RISKS YOU IDENTIFIED. THE RISK MANAGEMENT PLAN WILL DETERMINE WHAT CHANGES YOU MAKE TO ENSURE YOUR ePHI AND YOUR BUSINESS ARE SAFE FROM ALL REASONABLY ANTICIPATED THREATS.



# WHAT IS A RISK MANAGEMENT PLAN?

In the SRA, risk is identified, current security measures are evaluated, and the potential impact of a vulnerability being exploited/triggered is determined. A risk management plan takes all that information and turns it into a plan of action. It prioritizes the risks with the greatest impact, puts plans in place to mitigate the danger, implements those plans, then evaluates whether the risk is brought down to reasonable and appropriate levels.  The SRA and the risk management plan together serve as the foundation for compliance with the Security Rule. If you've performed a thorough SRA and created a comprehensive risk management plan, many later standards may be fulfilled in the process of implementing the plan and mitigating the identified risks.

**A COMPREHENSIVE RISK MANAGEMENT PLAN ALSO SERVES TO SATISFY SEVERAL HIPAA STANDARDS.**

164.308(a)(1)(ii)(B) – Risk Management: Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a).

164.308(a)(8) – Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operations changes affecting the security of [ePHI], that establishes the extent to which an entity's security policies and procedures meet the requirements of [the Security Rule].



**“RISK ANALYSIS AND RISK MANAGEMENT ARE THE FOUNDATION OF A COVERED ENTITY'S SECURITY RULE COMPLIANCE EFFORTS.”**



A person in a red jacket is climbing a steep, textured ice wall. The climber is positioned in the lower center of the frame, reaching up with their right hand. The ice wall is composed of large, irregular blocks of ice, creating a complex and challenging climbing surface. The background shows a bright blue sky with some white clouds, suggesting a high-altitude or mountainous environment. The overall scene conveys a sense of adventure, challenge, and overcoming obstacles.

# FOUR STEPS TO CREATING A RISK MANAGEMENT PLAN

In the SRA, risk is identified, current security measures are evaluated, and the potential impact of a vulnerability being exploited/triggered is determined. A risk management plan takes all that information and turns it into a plan of action. It prioritizes the risks with the greatest impact, puts plans in place to mitigate the danger, implements those plans, then evaluates whether the risk is brought down to reasonable and appropriate levels.

The SRA and the risk management plan together serve as the foundation for compliance with the Security Rule. If you've performed a thorough SRA and created a comprehensive risk management plan, many of the later standards may be fulfilled in the process of implementing the plan and mitigating the identified risks.

A comprehensive risk management plan also serves to satisfy several HIPAA standards.

**164.308(a)(1)(ii)(B)**—Risk Management: Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a).

**164.308(a)(8)**—Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operations changes affecting the security of [ePHI], that establishes the extent to which an entity's security policies and procedures meet the requirements of [the Security Rule].

# PRIORITIZATION

The first step of analyzing the data produced in the SRA is to prioritize which risks need to be addressed immediately and which can be addressed in the future. All risk eventually needs to be dealt with, but budgets, manpower, and immediate threats will all factor into how and when.

It's vital that senior management is involved in the risk management planning process. Mitigating risk to a reasonable and appropriate level may require considerable investment of both time and money. New hardware infrastructure or outside help from IT professionals may be necessary, and employees' time may be needed to create new policies and procedures and train staff. Even if the budget-makers aren't involved in the SRA, having them involved in the risk management plan will help to prioritize what needs to be handled first, and allow them to see why the investment is necessary.

WE CANNOT STRESS ENOUGH THAT WHILE COST IS ONE FACTOR TO CONSIDER IN YOUR MITIGATION STRATEGY, IT ALONE **CANNOT** BE USED TO JUSTIFY NOT MITIGATING RISK IF THE LIKELIHOOD OF A THREAT AND THE POTENTIAL IMPACT ARE SEVERE ENOUGH.

# MITIGATION

Once the risks are prioritized, the next step is to decide how to mitigate the possible danger. Just as with the rest of HIPAA, how this happens is determined differently by each company depending on the level of risk posed and the resources available.

What's important to remember is that the goal is not to eliminate risk all together. If it's possible to do so and still have a functioning and sustainable business, all the better, but for most businesses, the complete elimination of risk may be either too expensive or too prohibitive to actually continue fulfilling their core mission. The goal of mitigation is to reduce risk to a reasonable and appropriate level. Do all you can within your means to protect ePHI.





A comprehensive risk management plan is useless if it's not implemented. Failure to put the new policies and procedures to safeguard ePHI into action throughout your company can result in the vulnerabilities you identified being exploited: exposing ePHI, your company losing trust, and incurring serious fines.

Implementation needs to occur at all levels of your business, from documenting the newly created policies and procedures, to infrastructure investments, to checking the settings on hardware you identified as a risk. According to [NIST SP 800-39](#),

“THE OBJECTIVE IS TO INSTITUTIONALIZE RISK MANAGEMENT INTO THE DAY-TO-DAY OPERATIONS AS A PRIORITY AND AN INTEGRAL PART OF HOW ORGANIZATIONS CONDUCT OPERATIONS . . . RECOGNIZING THAT THIS IS ESSENTIAL IN ORDER TO SUCCESSFULLY CARRY OUT [BUSINESS] MISSIONS IN THREAT-LADEN OPERATIONAL ENVIRONMENTS.”

NIST is talking about IT operations, but the same is true to all threats to ePHI. A culture of avoiding or mitigating risk at every level can produce a working environment that protects ePHI and strives to maintain security measures. Remember, the risk management plan is essentially a plan of action that must be put into practice to be successful.

## EVALUATION

Implementing your risk management plan won't protect ePHI if, ultimately, the mitigation strategy you chose doesn't work as expected. That's why evaluating the success of your risk management plan after implementation is important. Once in place, you may find that what you thought would mitigate the risk hasn't done so, or hasn't done it as well as necessary to bring the danger down to reasonable and appropriate levels. Or you may find that while it does mitigate risk, it also causes severe difficulties in the day-to-day operations of your business. In these cases, another strategy may be more successful for your business in the long run.

§164.308(a)(8) also requires covered entities to “perform a periodic technical and nontechnical evaluation . . . in response to

environmental or operations changes . . . that establishes the extent to which an entity's security policies and procedures meet the requirements of [the Security Rule].” This means that subsequent SRAs need to be performed and your risk management plan re-evaluated whenever there are major changes to your business or IT infrastructure that could affect ePHI.

Like we mentioned in section three of this ebook, documentation is a constant part of compliance with the Security Rule, and the risk management plan is no different. Having a clear record of what you planned, when and how you implemented the plan, and the success or failure of those actions are necessary not only for your own future use but also in case you're audited.



**RISK MANAGEMENT DOESN'T JUST HAPPEN AT THE OFFICE. VET ALL VENDORS AND SERVICE PROVIDERS FOR POTENTIAL RISK AND VERIFY THEIR DUE DILIGENCE BEFORE PARTNERING WITH THEM.**

## THE CYCLE NEVER ENDS

The most important thing to remember about risk is that it never ends and is always finding new ways to threaten your business. You have to keep moving right along with it. Risk management is a continuous cycle of analyzing risk, implementing a plan to fix it, determining if that plan worked, and repeating.

For some businesses, performing an SRA and updating a risk management plan might be an annual activity as part of their HIPAA compliance. Other businesses that have fewer risks and fewer changes to the business may decide to wait two or three years between SRAs. It all depends on what is reasonable and appropriate for your organization. Just don't stop moving through the cycle of risk management. Danger doesn't stop changing, and neither should you.



# PLAN FOR THE WORST

**N** NO ONE LIKES TO THINK THEY'LL SUFFER A DISASTER, A RANSOMWARE ATTACK, OR A DATA BREACH, BUT HOPE ISN'T ENOUGH TO SATISFY HIPAA. HIPAA EXPECTS YOU TO PLAN, PREPARE, TEST, AND BE READY FOR ANYTHING THAT COULD DISRUPT YOUR ePHI AND AFFECT PATIENT CARE. ■■■■■

**SECURITY STANDARD §164.308(A)(7): CONTINGENCY PLAN IS AN UMBRELLA TERM FOR A NUMBER OF MORE SPECIFIC PLANS THAT ARE MEANT TO ENSURE THE AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY OF ePHI IN THE EVENT OF A DISASTER OR OTHER MAJOR SECURITY INCIDENT. NON-ELECTRONIC PHI IS COVERED BY THE PRIVACY RULE AND MOST CYBER INSURANCE PLANS ALSO REQUIRE SOME DEGREE OF BUSINESS CONTINGENCY PLANNING.**

# CONTINGENCY PLANS

## FIRST THINGS FIRST

**Before you can start** making plans to keep your business going during and after a disaster or cybersecurity incident, you first need to know what parts of your business, hardware, software, and data are critical to operations and security. HIPAA requires this in implementation specification §164.308(a)(7)(ii)(E): Applications and Data Criticality Analysis. But don't let its position after the contingency plans fool you. This needs to be done first and foremost. ■■■■■ Even though §164.308(a)(7) only references assessing "specific applications and data," if you are implementing business-wide contingency plans, you'll want to go through all

your daily operations and vital processes to determine what you can't do a day's worth of business without and what you could leave for when your world is no longer upside down. Without this information, you won't be able to create the plans necessary to fulfill the following implementation specifications.

## THE BIG FOUR

One thing to remember about the plans listed below is that they don't have to be completely isolated from each other. You might find combining pieces together (such as lists of vendors, hardware, software, etc.) is more practical than listing them in each plan separately. What's important is that employees are trained, know what they are responsible for, and where to access this information in an emergency situation. There's no use making a plan if no one uses it.

THE  
QUESTION  
IS NO  
LONGER *IF*  
SOMETHING  
WILL  
HAPPEN, BUT  
*WHEN.*



## DATA BACKUP PLAN §164.308(A)(7)(ii)(A)

ESTABLISH AND IMPLEMENT PROCEDURES TO CREATE AND MAINTAIN RETRIEVABLE EXACT COPIES OF ELECTRONIC PROTECTED HEALTH INFORMATION.

### WHAT DOES IT DO?

Your data backup plan is one of your most vital recovery plans. It provides you with assurances of data integrity and availability in emergency situations. For healthcare facilities directly caring for patients, data loss or network failure could mean the inability to treat patients. All ePHI must be backed up, preferably in a place that won't suffer the same disaster as your facility, such as in cloud storage or in a separate secure location.

Your data backup plan should include who is responsible for maintaining the backups, verifying all data is being backed up, testing that backups can be retrieved, and who to contact when backups are needed.

A DATA BACKUP PLAN IS ALSO ONE OF THE BEST DEFENSES AGAINST RANSOMWARE.

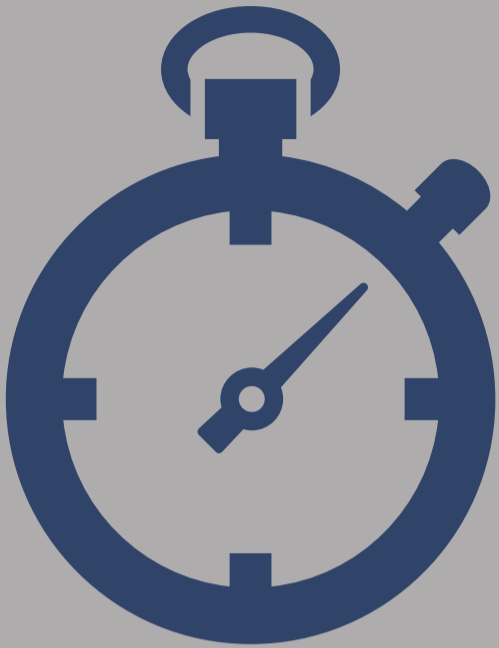
READ MORE ABOUT THAT [HERE!](#)

“FOLLOWING STANDARDIZED RESPONSES SHOULD MINIMIZE ERRORS, PARTICULARLY THOSE THAT MIGHT BE CAUSED BY STRESSFUL INCIDENT HANDLING SITUATIONS.” – [NIST](#)

### WHEN DOES IT GO INTO EFFECT?

You should make this a priority. Your data backup plan needs to be up and running **before** an emergency strikes.





## DISASTER RECOVERY PLAN §164.308(A)(7)(II)(B)

ESTABLISH (AND IMPLEMENT AS NEEDED) PROCEDURES TO RESTORE ANY LOSS OF DATA.

### WHAT DOES IT DO?

The complexity of a disaster recovery plan depends on how much of your business you choose to include. More comprehensive business-wide plans would include other data vital to the company that isn't specifically ePHI.

A disaster recovery plan should include the hardware, software, backups, environment, vendors, business associates, etc., necessary to recover data lost in a disaster or cybersecurity incident. It also covers the people responsible for coordinating and performing all disaster recovery efforts. Employees assigned in this plan should be trained and ready to fulfill their duties in the event of a disaster.

A PLAN IS NO GOOD IF NO ONE  
KNOWS WHERE IT IS OR WHAT THEY  
ARE RESPONSIBLE FOR.

TRAINING IS KEY!



### WHEN DOES IT GO INTO EFFECT?

A disaster recovery plan helps you recover lost data and infrastructure **after** a disaster or cybersecurity incident has occurred.

# EMERGENCY MODE OPERATIONS PLAN

## §164.308(A)(7)(II)(C)

ESTABLISH (AND IMPLEMENT AS NEEDED) PROCEDURES TO ENABLE CONTINUATION OF CRITICAL BUSINESS PROCESSES FOR PROTECTION OF THE SECURITY OF ELECTRONIC PROTECTED HEALTH INFORMATION WHILE OPERATING IN EMERGENCY MODE.



## WHAT DOES IT DO?

This plan could also be called a continuity of operations plan. Its intent is to keep your business or facility operating at a level necessary to ensure patient safety and ePHI security the moment a disaster hits. Downtime can not only cost a lot of money, but can be detrimental to facilities actively caring for patients.

By having the procedures in place for any number of emergency situations, employees can react immediately, know who to contact, how to bring critical business processes back online, and maintain the necessary security and privacy standards required by HIPAA. A good emergency mode operations plan

should have contact names, numbers, first response expectations, and anything else an employee would need to recover critical operations in the first 12-36 hours.

More than the other plans, having done a thorough and accurate criticality analysis is vital to a successful emergency mode operation plan. You need to be aware of what you need to restore and in what order it needs to be restored to effectively continue with daily operations as best you can. Failure to do a proper criticality analysis can waste time and resources by focusing recovery efforts on functions that aren't immediately necessary.

A CLEAR CHAIN OF COMMAND DURING EMERGENCY SITUATIONS KEEPS STAFF AND PATIENTS SAFE.

MAKE SURE EVERYONE KNOWS WHAT TO DO BEFORE DISASTER STRIKES!

## WHEN DOES IT GO INTO EFFECT?

An emergency mode operations plan should be implemented **during** a disaster to keep the business going, and, in the case of healthcare facilities, to keep patients safe and cared for appropriately.



# BUSINESS CONTINUITY

## WHAT DOES IT DO?

You'll notice that there is no implementation specification that goes along with this plan. The Security Rule doesn't specifically require a business continuity plan, but it can be a useful addition to a set of contingency plans.

While the other plans all focus on what happens during or immediately after an emergency situation to keep your business running, a business continuity plan focuses on getting you back to where you were before the disaster. What are the lower priority vendors or clients that you might have missed contacting already? Do you know all the hardware and software that needs to be replaced or recovered? Think of it as the long-haul plan that doesn't let you forget about the little things. Disasters are stressful, and a good business continuity plan can keep you on track through the mental fatigue that can set in after a disaster.

---

**DON'T LET THE LITTLE THINGS SLIP THROUGH THE CRACKS AS YOU WORK TO RECOVER YOUR BUSINESS.**



## WHEN DOES IT GO INTO EFFECT?

Business continuity plans help you bring your entire business back to normal day-to-day operations **after** a disaster occurs and the crisis period is over.



# INCIDENT RESPONSE

There are many different kinds of cybersecurity incidents that could affect your business. While all incidents are major problems when they occur, you may not require the full emergency responses planned out above. In these cases, individual plans geared directly to cyber problems can be useful tools. ■ Depending on your risk, you may want more than the two plans below, but if you're covered by HIPAA, these are important ones to include with your disaster management plans. The better prepared you are for an incident, the safer you can make your data and the faster you can recover from an attack.



---

“COMPANIES THAT IDENTIFIED A BREACH IN LESS THAN 100 DAYS SAVED MORE THAN \$1 MILLION AS COMPARED TO THOSE THAT TOOK MORE THAN 100 DAYS. SIMILARLY, COMPANIES THAT CONTAINED A BREACH IN LESS THAN 30 DAYS SAVED OVER \$1 MILLION AS COMPARED TO THOSE THAT TOOK MORE THAN 30 DAYS TO RESOLVE.”

— [2018 COST OF A DATA BREACH STUDY, PONEMON INSTITUTE](#)

# DATA BREACH RESPONSE PLAN

While a breach is any impermissible use or disclosure of PHI, a data breach response plan focuses on ePHI specifically. It lays out how to secure your systems after a breach, who to contact if you need more support, what to do once the threat is identified and fixed, and who must be notified of a breach of ePHI or other personally identifiable information (PII). (Remember, improper access to [properly encrypted data](#) isn't a breach.) The [FTC has a good outline](#) for what to incorporate into your data response plan, and the [HHS thoroughly explains](#) all the requirements of a breach under HIPAA.



THE BLACK  
MARKET VALUE  
OF A SINGLE  
HEALTHCARE  
RECORD  
AVERAGED

**\$250**

IN 2018.

([The Value of Data](#))

## RANSOMWARE ATTACK RESPONSE PLAN

The criticality of care facilities combined with the [black market price](#) of ePHI makes the healthcare industry a prime target for ransomware and other cyber attacks. Like most cyber attacks, ransomware deals two-fold damage, from the recovery itself to the subsequent breach notifications that must follow. (Remember, unless you can prove that ePHI has not been accessed due to safeguards in place, it's a breach. For more on ransomware and HIPAA, see the [HHS's Fact Sheet](#).)

A ransomware attack response plan sets up the procedures your employees should take in the event of a ransomware attack, such as steps to quarantine an infected machine, who to contact, and what not to do. It should also have procedures for technicians and management on how to secure the network, purge the system, recover lost data (per the data backup plan), and notify required parties. Also include the contact information of the law enforcement department to report the attack to, whether that is local, state, or federal. (For more information see the Department of Justice's guide, "[How to Protect Your Networks from Ransomware](#).")





# DISASTER RECOVERY PLAN

## TEST! TEST! TEST!

Test your contingency plans routinely and make sure all your employees are trained and know where to find the plan in emergency conditions. A plan no one knows about or can find is a plan that won't be implemented.

Include contingency plans in your annual and new-hire training. Make sure all your employees can find the plans and that they know what they are responsible for. Educate everyone on who's in charge during emergency situations so that plans can be implemented quickly and efficiently. It will save you time, money, and headaches when the worst happens.

# GETTING STARTED



For those of you tackling HIPAA for the first time or those whose current HIPAA compliance program isn't doing enough, here are a few tips to help you start the process.

**Know what you have**—Starting a HIPAA compliance program begins with determining what PHI and ePHI you have, what programs or processes access that information, and what policies or safeguards are already in place to protect it. Without knowing that, you can't know what needs to be fixed.

**Perform the SRA first**—It's the first security standard for a reason. A complete and thorough Security Risk Analysis is critical to compliance, and you'll find that during the SRA process you'll address many of the other standards in the Security Rule. If you don't feel you can perform this on your own, it may be beneficial to call in an outside consulting company to help you.

**Document everything**—Get used to this right away. You must not only become compliant, but you need to prove that you are compliant, and that is done through documentation. Be careful you don't fall into the trap of "paper compliance," where you have the documentation but fail to follow through in everyday practice. A policy is useless if it's not implemented.

**Accept that it's a process**—Compliance doesn't happen overnight. From the SRA to the documentation to the evaluations, compliance takes time. It is a continuous process of monitoring and updating to ensure the privacy and security of PHI.

**Get everyone on the same page**—HIPAA training needs to happen from top to bottom. This helps create

a culture of compliance that will make ongoing compliance efforts easier. If those in leadership positions understand why it's important to be HIPAA compliant, appropriate policies and procedures can be created and the budget adjusted according to needs. When employees know the rules to ensure the confidentiality, integrity, and availability of PHI, there is less chance that an avoidable breach will happen.

There is no one prescriptive way to go about HIPAA compliance. HIPAA is designed to be vague enough that any size or type of business can adopt the same requirements, which gives each business a lot of freedom but also greater responsibility. With that said, what does HIPAA compliance mean for you?

## TIPS FOR BEGINNERS



# RESOURCES

KNOWING WHERE TO GO FOR INFORMATION CAN ASSIST ANY COMPLIANCE OFFICER IN THEIR EFFORTS TO BECOME HIPAA COMPLIANT. BELOW IS A COLLECTION OF LINKS TO ALL OF THE RESOURCES FOUND THROUGHOUT THIS EBOOK.

## HIPAA

<a href="#">THE HITECH ACT</a>	<a href="#">THE OMNIBUS RULE</a>	<a href="#">HHS BREACH DATABASE</a>	<a href="#">PUBLIC LAW 104–191 AUG. 21, 1996</a>
--------------------------------	----------------------------------	-------------------------------------	--

## INTRODUCTION TO THE SECURITY RULE

<a href="#">HHS SECURITY SERIES</a>	<a href="#">NIST INTRODUCTORY GUIDE TO HIPAA</a>
-------------------------------------	--

## SECURITY RISK ANALYSIS

<a href="#">MYTHS OF THE SRA</a>	<a href="#">SRA TOOL</a>	<a href="#">SRA VIDEOS</a>	<a href="#">PRIVACY AND SECURITY TRAINING GAMES</a>
<a href="#">HHS SECURITY SERIES - SRA</a>	<a href="#">ONC GUIDE TO PRIVACY AND SECURITY OF EPHI</a>	<a href="#">HHS GUIDE ON SRA</a>	<a href="#">NIST MANAGING INFORMATION SECURITY RISK</a>

[NIST GUIDE TO CONDUCTING RISK ASSESSMENTS](#)

# RESOURCES

## CONTINGENCY PLANS

[HHS EMERGENCY  
PREPAREDNESS](#)

---

[COST OF DATA  
BREACH STUDY](#)

---

[HHS ENCRYPTION  
GUIDANCE](#)

---

[HOMELAND SECURITY  
CYBERSECURITY  
INSURANCE](#)

---

[HHS BREACH  
NOTIFICATION](#)

---

[HHS RANSOMWARE  
AND HIPAA](#)

---

[DOJ HOW TO  
PROTECT FROM  
RANSOMWARE](#)

---

# ABOUT ANDERSON TECHNOLOGIES

WE HOPE YOU FOUND THIS HIPAA BEGINNER'S GUIDE USEFUL. GETTING STARTED IS OFTEN THE HARDEST PART OF ANY PROJECT, BUT WITH A LITTLE HELP YOU'LL BE HIPAA COMPLIANT IN NO TIME.



Are you ready to get started but need some assistance? Perhaps you're frustrated by assessments and access or looking for a trusted partner to provide feedback? Anderson Technologies can help. Our in-house expertise with the technical requirements of HIPAA combined with our strategic partnership with a nationally recognized HIPAA-expert can streamline this process and get you where you need to be.

LEARN MORE ABOUT OUR HIPAA SERVICES



## HAVE ANY QUESTIONS?

The team at Anderson Technologies is happy to discuss any questions you have or schedule a time to go over your HIPAA security needs. Contact us about our HIPAA services today at [info@andersontech.com](mailto:info@andersontech.com) or [314.394.3001](tel:314.394.3001). We're here to help!



Get Hip to HIPAA: A Beginner's Guide to HIPAA Compliance  
<https://andersontech.com> | [info@andersontech.com](mailto:info@andersontech.com) | [314.394.3001](tel:314.394.3001)