

Fulfilling Security Officer Duties in Mental/Behavioral Health Group Practice

Roy Huggins, LPC NCC



Our Educational Objectives

- Orient to the duties and regulatory environment of the HIPAA Security Officer role
- Describe, at a high level, the set of tasks necessary for establishing and running a HIPAA-compliant security risk management program
- Explain to practice staff members the value and necessity of a HIPAA-compliant security risk management program

Other Courses in This Program

The Person Centered Tech Security Officer Training Program:

- HIPAA Security Compliance in Mental Health, a Guided Reading (1 CE credit)
 - Referenced throughout this course as “HIPAA Reading.”
- **Fulfilling Security Officer Duties in Mental/Behavioral Health Group Practice**
 - This course
- Engaging in HIPAA Security and Digital Confidentiality as a Mental Health Professional (9 CE credits)
 - References throughout this course as “HIPAACore”

Module 1: The Security Officer's World



Unit 1: A Security Officer's Responsibilities



Inside the Practice (Internal) Responsibilities

- The practice is the **covered entity**. (*HIPAA Reading Unit 1*)
 - Importantly, individual clinicians in the practice are *not* the covered entity. The practice is the entity which is responsible for compliance!
- You are the primary officer in charge of ensuring it remains in compliance with HIPAA's security risk management standards.
- There are 18 Security Rule standards and 36 "implementation specifications."

Complying with HIPAA's Security standards means developing a risk management program for the practice which 1) continuously maintains the standards, and 2) prevents security breaches or complaints.

Outside the Practice (External) Responsibilities

- Lead the investigation of **security incidents**. (*HIPAA Reading Unit 4; HIPAACore Mod 5*)
 - This is both internal and external, but it relates to how the practice interfaces with the outside world. Security incident investigations often involve clients, and can also involve law enforcement (especially when the security incident is a theft.)
- Respond to auditors and investigators.

Delegation -- Yes, You Can!

- The SO's job involved a lot of different activities.
- It is perfectly fine to delegate.
 - Outside of very small practices, it is expected that you will assign most day-to-day security tasks to other staff members.
- Other side of the coin: you need to take responsibility if something is not done or is not done correctly.



“The Buck Stops Here”

Assigned Responsibilities

- Assigning security responsibilities to members of leadership is a HIPAA Security standard.
- As the SO, you are taking the top-level responsibility for creating and maintaining the practice's security risk management program.
- Others (or you) wear related-but-different hats:
 - Privacy Officer
 - Technical / IT Officer
 - Other “officers” as needed

Assigned Responsibilities: What the SO Needs

- As the Security Officer, you need **authority** and **resources** to:
 - Create and enforce security policies and procedures
 - Acquire and develop new technical resources for the staff when they need them
 - E.g. phone services, email services, shredders, locking boxes, etc.
 - Be the final decider on what electronic systems are acceptable to the practice and what are not
 - Yes, even the practice's owner or executive director needs your sign-off before making decisions or setting up systems that impact the practice's security
- The practice owner or executive director generally needs to assign you this authority and these resources.
 - If they are hesitant or unsure, have them speak with someone at Person Centered Tech.

Unit 2: Compliance Authorities

**PERSON
CENTERED
TECH**



Federal Authorities

- **The Office of Civil Rights (OCR)**
 - An office under Health and Human Services
 - “The HIPAA People.” The OCR writes and enforces HIPAA rules.
- Others you may have to comply with:
 - For EHR Meaningful Use: The Office of the National Coordinator for Health Information Technology (ONC.)
 - If you are pursuing or maintaining incentives for using an EHR, the ONC oversees that program. The requirements of meaningful use, etc. overlap with HIPAA but are *not* the same as HIPAA.
 - For Medicare: The Center for Medicare and Medicaid Studies (CMS.)
 - If the practice accepts medicare or medicaid, you may need to comply with some rules from CMS. They may require you to comply with HIPAA’s security standards. They are *not* the enforcers of HIPAA, however. That is the OCR.
 - For substance use treatment centers: 42 CFR Part 2.
 - This is a special rule for certain entities which perform substance use treatment. In some ways, 42 CFR Part 2 actually conflicts with HIPAA. 42 CFR Part 2 is primarily the responsibility of Privacy Officers.

State and Local Authorities

- **The State Attorney General (AG)**
 - The states' attorneys general are empowered to enforce HIPAA in their states.
 - Yes, when the state AG enforces HIPAA, they are still enforcing the federal regulation itself.
- Others you may have to comply with:
 - The state AG, but enforcing various state laws -- including state data breach laws.
 - Example 1: Texas has a state law which requires all practices perform a security risk analysis and that all licensed clinicians be trained in HIPAA and any other privacy laws which apply to them.
 - Example 2: California's state data breach rule allows entities a lot less time to investigate security incidents than HIPAA does.
 - Licensing boards for the practice's clinicians.
 - Any other state or local powers which may be.

Unit 3: Security Officers: A Year In The Life

PERSON
CENTERED
TECH



Activities You Will Always Do Over the Year

- Risk Analysis (*HIPAACore Mod 8 Unit 3*), and Policies & Procedures
- Staff Onboarding and Offboarding (*HIPAACore Mod 2 Unit 8*)
- Staff Training (*HIPAACore Mod 2 Unit 8*)
 - Formal trainings
 - Security reminders
- Regular Security Activities (*HIPAACore Various*)
 - Backups, password changes, access log reviews, and more!
- Catalogs and Logs
 - Asset and staff catalogs
 - Security activity logs

Sometimes Activities -- “The Fun Parts”

- Selecting technical services and equipment for the practice
- Vetting services to be sure they fit with the practice’s security risk management program (*HIPAACore Mod 8 Unit 2*)
- Coming up with solutions to make sure staff have the resources they need to do their jobs without compromising practice security

Sometimes Activities -- “The Less Fun Parts”

- Correcting staff behavior (*HIPAACore Mod 2 Unit 8*)
 - HIPAA’s standards require the practice have a policy defining “sanctions” for staff members who violate policies.
 - Sanctions need not always be punishments. Most HR experts agree that it is better to help a staff member understand what they did wrong and help them correct their mistake(s) going forward.
 - Sometimes, however, termination of employment may be called for -- especially in the case of egregious violations of security policies.
- Investigating and acting on security incidents (*HIPAACore Mod 5*)
 - Investigating reported incidents.
 - Performing breach notification, if necessary

Module 2: The Risk Management Program



Unit 1: The Value and Goals of Your Security Risk Management Program



The Value and the Goals of a Good Program

- Protects clients and staff from harm
- Supports staff in having a clear structure and resources for the technical logistics of their work
- Prevents complaints from clients
 - Or at least it can prevent their complaints from having legal merit
- Prevents security breaches
- Responds effectively and resourcefully to security incidents and breaches

Communicating the Value and Goals to Staff

- Emphasize that mental health clinicians have always taken client privacy more seriously than any other health care profession -- this program is not so different from that same attitude of professionalism.
- Security and compliance are both akin to self-care for the practice and for its clinicians. Keeping the doors open and free of drama is good for client care.
- The program provides structure and guidance in a realm that may otherwise be very “willy nilly.” The SO is a person they can go to with questions and concerns, and to get needs met.
- If something goes awry, the practice is much more likely to be prepared and to respond adaptively and effectively.

Two Models for Conceptualizing Your Program

1. **“Keep It In The Circle”** -- a model that provides a clear idea of what your program’s main objectives and goals are. You can share this model with the staff and enroll them in helping you to maintain it.
2. **The Cycle of Security Activities** -- a high-level description of the processes necessary for HIPAA compliance, presented temporally and logically so that you can conceptualize how your program flows over time. This one is more for you and other members of the practice’s leadership. It is less useful for helping to enroll staff in maintaining the program.

Unit 2:

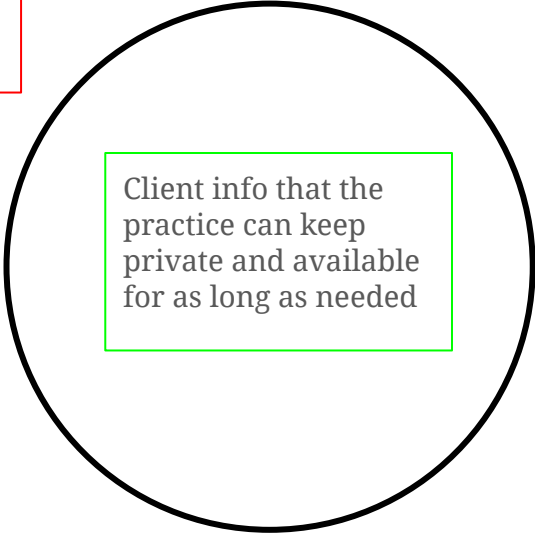
The Person Centered Tech Strategic
Model for Security Risk Management
Leadership:

“Keep It In The Circle”



Why “Keep It In the Circle”?

Client info that the practice cannot protect and to which the practice has no access

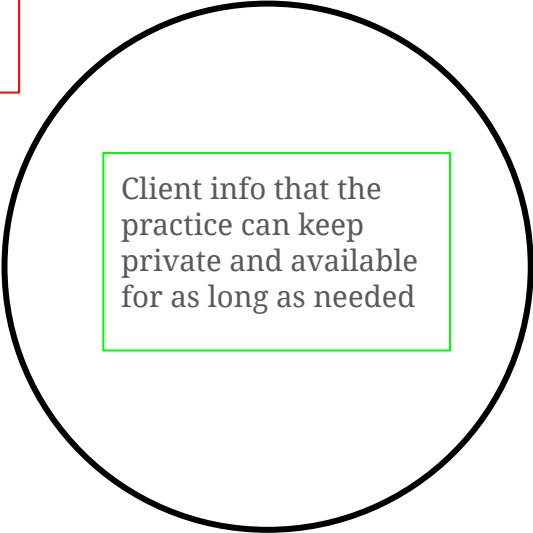


Client info that the practice can keep private and available for as long as needed

- Provides a way of conceptualizing the practice and its PHI that is simple and easy to understand.
- It provides a “north star” for the SO, so that you can more easily know what your risk management program is aiming for. That helps you know how to make decisions when the need arises (i.e. you always know that whatever path you choose should be one that “keeps it in the circle.”)
- It is something that can be taught to the staff, as well! They can also understand what “the circle” is and engage in maintaining its integrity.

What is “The Circle”?

Client info that the practice cannot protect and to which the practice has no access



Client info that the practice can keep private and available for as long as needed

- Maintaining the secure “circle” means:
 - Knowing where protected health information is
 - Maintaining the confidentiality of info
 - Making sure info is available to the practice for as long as it needs to be maintained.
- Services have a Business Associate Agreements between the service provider and *the practice* (not individuals who work for the practice)
- Staff are **not** using personal or personally-obtained services that are outside the practice’s control and access

Concept: What is Protected Health Information?

PHI that the practice cannot protect and to which the practice has no access

PHI that the practice can keep private and available for as long as needed

Protected Health Information (PHI) =
(HIPAACore Mod 2 Unit 2)

Health Information
(HIPAACore Mod 2 Unit 2)

+

Personally Identifying Information
(HIPAACore Mod 2 Unit 5)

Concept: What is a Security Breach?

PHI that the practice cannot protect and to which the practice has no access -- **and may be disclosed without authorization or misused without the practice knowing it!**

PHI that the practice works to safeguard from unauthorized disclosure or misuse



Security Breach =
(HIPAA Core Mod 5)

Unauthorized Disclosure of PHI
(HIPAA Core Mod 5)

or

Misuse of PHI
(HIPAA Core Mod 5)

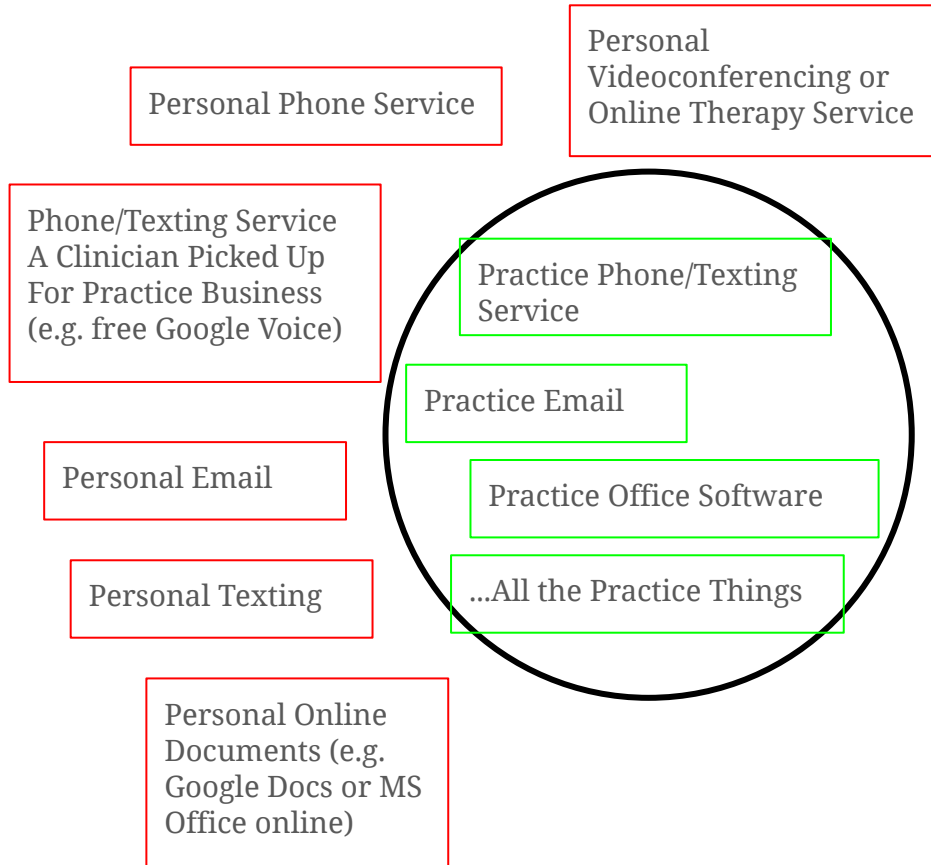
Objective: Know Where Your PHI Is

PHI that the practice cannot protect and to which the practice has no access

PHI that the practice can keep private and available for as long as needed

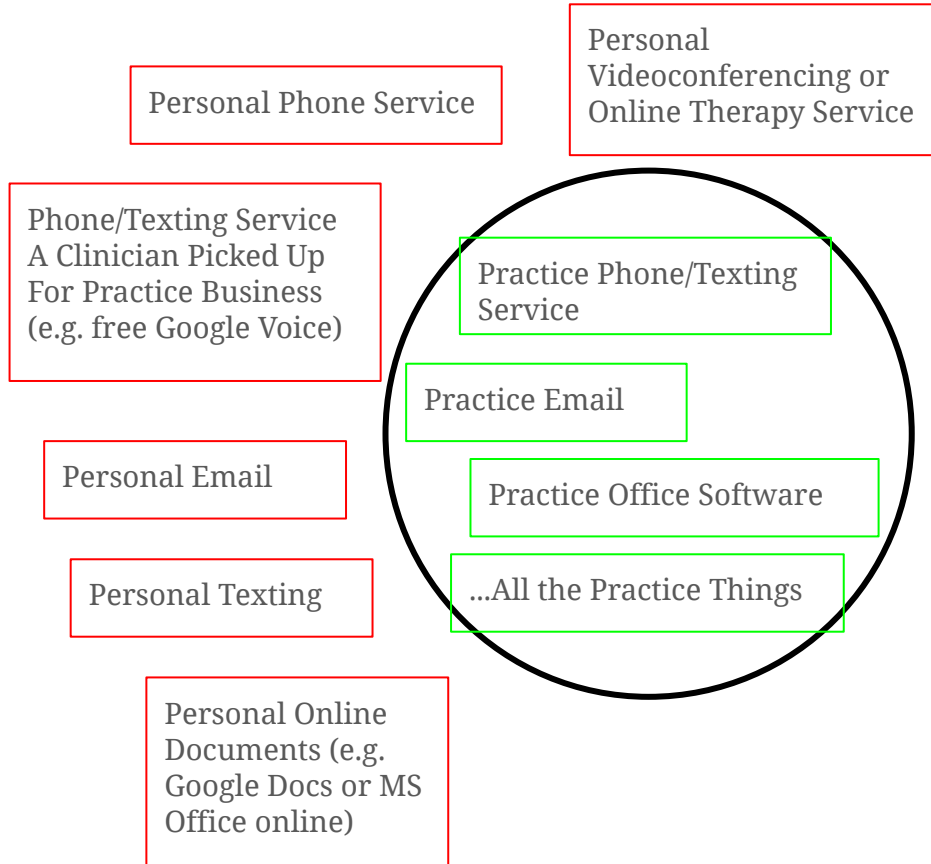
- You need to be able to describe what devices or services handle all the practice's PHI. *(HIPAA Core Mod 8 Unit 1)*
- If you discover PHI in a place you didn't know about, you need to take corrective action.
 - E.g. when staff members call clients, they need to use a practice-supplied phone service. If you discover a clinician using their personal phone service, you've discovered that PHI is being created "outside the circle." You need to correct the staff member's behavior so that they use the practice's phone service.
- *Once you find where your info is, the next step is to make sure it's safe there or move it somewhere that is safe for it.*

Objective: Know Where Your Assets Are



- As part of compliance, you need to have a catalog of all the practice's assets that handle PHI:
 - Computers, smartphones, copiers, thumb drives, etc.
 - Filing cabinets, shredders, etc.
 - People who work in the practice
 - Services that work for the practice:
 - Groups of people like billing services
 - Groups of people + server computers like email services, phone and texting services, practice management/EHR services, etc.
- A comprehensive risk analysis will include making sure your asset catalog is thorough and includes everything.
- In the modern world, you may need to spend time differentiating between the practice's assets and the personal assets of staff members.
 - Bring Your Own Device (BYOD) is very common and needs to be managed well -- but can be used!

Goal: “Keep It In The Circle”



Keeping it in the circle means:

- Every scrap of PHI handled by the practice is kept in a practice asset.
- PHI is never outside a practice-controlled asset or practice-approved asset (e.g. registered BYOD devices.)
- Services are properly brought into the circle -- with HIPAA, that generally means Business Associate Agreements with the service providers.
- All the practice’s systems are set up so they don’t “leak” or “forget” information.
- Policies and procedures protect the confidentiality, integrity, and availability of PHI in the circle

Circle Specifics: Keeping Staff Supported

- Make sure the practice supplies proper gear, services, or training for everything staff members need to do their jobs.
- If you don't, they will take PHI outside the circle in order to do their work.
 - Sometimes this means new systems are needed, sometimes it means training on the existing systems is needed.

Are therapists texting with clients even after someone told them not to?

It sounds like they either need training on how to avoid texting, or (more likely), they need a way to do texting with clients that keeps those text messages in the circle.

Maybe that's a secure texting app. Or maybe that's a practice-supplied phone service -- with classic SMS texting -- combined with clients' signed requests for those nonsecure SMS text messages (*HIPAACore Mod 4 Unit 3*).

Collaborate with the clinicians on their needs, perform a risk analysis, look at possible solutions, do a cost-benefit analysis of potential solutions, then meet the staff members' needs for providing service to clients while still maintaining the integrity of the circle.

Circle Specifics: Ensure Services Don't "Forget" PHI

- Services you use may delete information over time.
 - Some info, like activity logs, is only retained for a period of time.
 - When a staff member leaves the practice and their account is closed, the service "forgets" all the info associated with their account.
 - E.g. if using G Suite or MS 365, you need the level of service wherein they retain all information that ever passes through them, even if staff members leave and their accounts are cancelled.
 - E.g. some secure email services (like Gmail Confidential Mode) destroy the secure messages after a period of time.
- You will need to make sure your services are set up to retain information without ever "forgetting" it.

What examples of potential PHI "forgetting" can you think of in your practice?

Circle Specifics: Ensure Services Don't "Leak" PHI

- Services and gear you use may cause information to automatically “leak” or get synchronized to places outside the circle.
 - E.g. don't allow staff to set up their practice email to auto-forward to their personal email. You might be able to prevent this with a setting in the email service, or it might have to be a purely behavioral policy.
 - E.g. don't allow staff to share Google Docs or MS 365 Office files with people outside the practice unless the practice has an intentionally-designed process for doing so securely. Once again, you might be able to do this with technical policies or it might have to be done with behavioral policies.
 - E.g. iPhones and iPads like to synchronize data with the owner's personal iCloud account. The BYOD policy needs to instruct staff member not to allow this feature to “sync” and practice information with the staff member's personal iCloud.
- You will need to make sure your services and gear are set up to prevent “leaking.”

What examples of potential PHI “leaking” can you think of in your practice?

Circle Specifics: Ban Bring Your Own Service (BYOS)

- Policies should explicitly state that staff may not use their own services to conduct practice business.
 - Examples of personal services: one's own phone service (i.e. the service they have on their personal phone), their own texting or a texting service they picked up just for talking to clients, a personal email service, and much more.
 - It may take some education to help staff understand what a personal service is and why it isn't wise to use them.
- One exception: using personal cellular data, purely as an Internet connection, should be permitted and encouraged as an alternative to using unknown WiFi (*HIPAACore Mod 6 Unit 4*)
- Important: personal *services* are different from personal *devices*.

What examples of BYOS can you think of in your practice?

Circle Specifics: Manage Bring Your Own Device (BYOD)

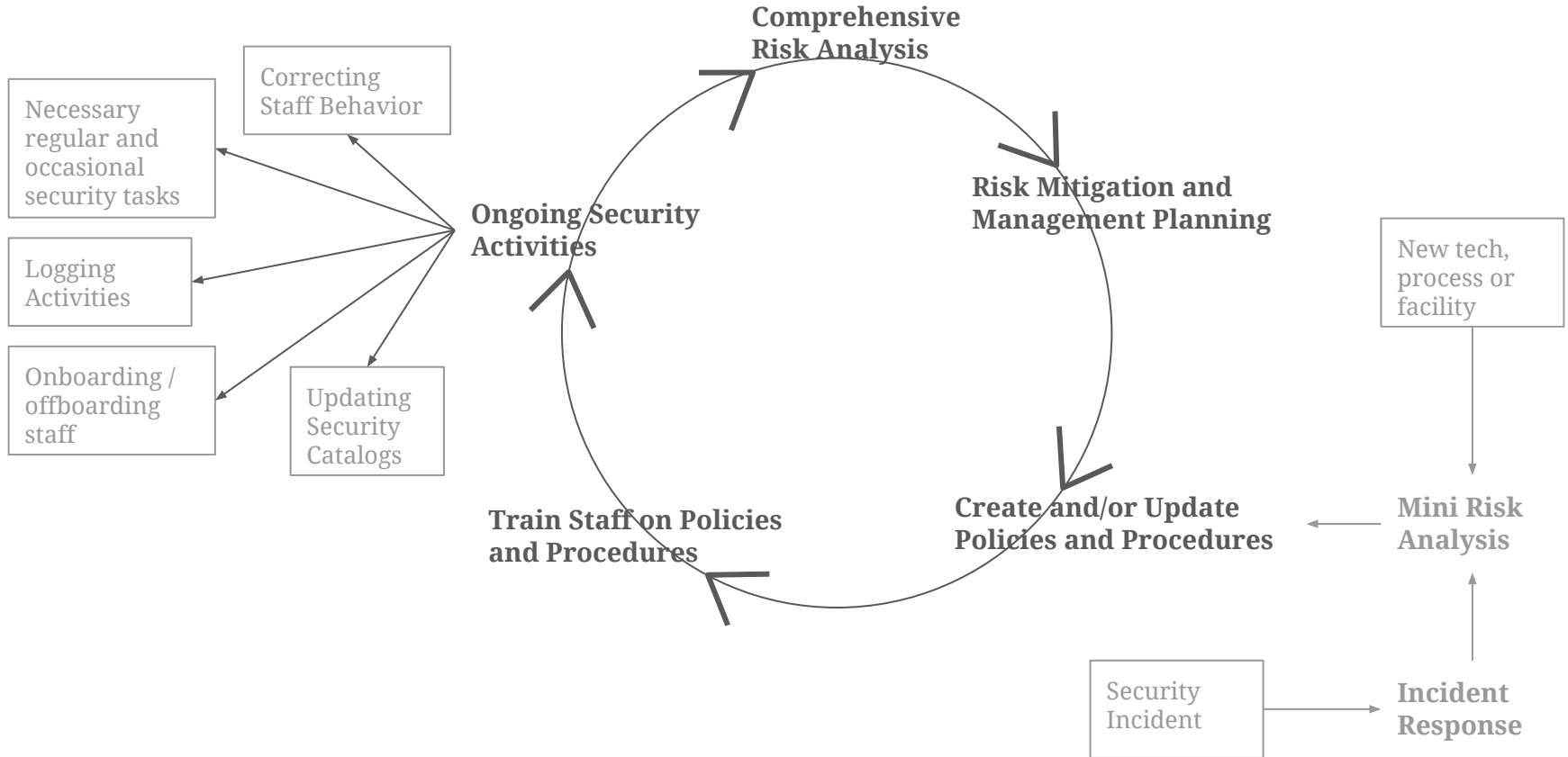
- Set up a program to have staff members register personal devices they wish to use in the service.
- Devices must be “hardened” according to a rubric set in practice policy, which includes rules about permitted software, permitted WiFi, and other measures necessary to prevent the devices from becoming a way for PHI to get compromised by thieves, viruses, curious family members, and others.
 - Develop your own BYOD rules or use the program available for group practices through Person Centered Tech.
- Secured devices may be registered for use, and then later unregistered. Unregistered devices need to be “scrubbed” of PHI. Registration and unregistration needs to be logged.
- Some practices allow all personal devices, while some only allow smartphones as BYOD devices.

What examples of BYOD can you think of in your practice?

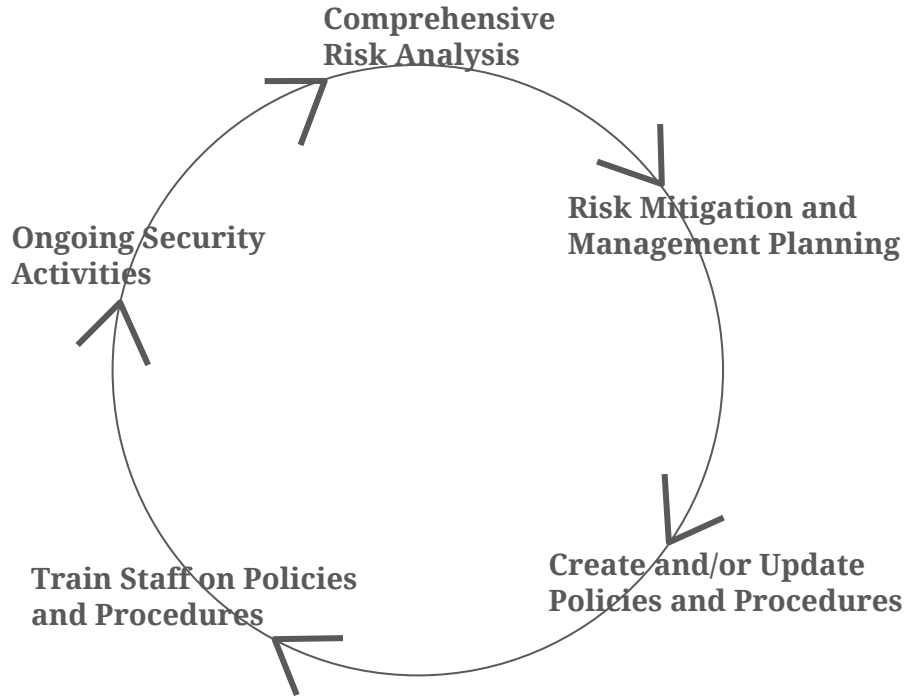
Unit 3: The Cycle of Security Activities



The Cycle of Security Activities

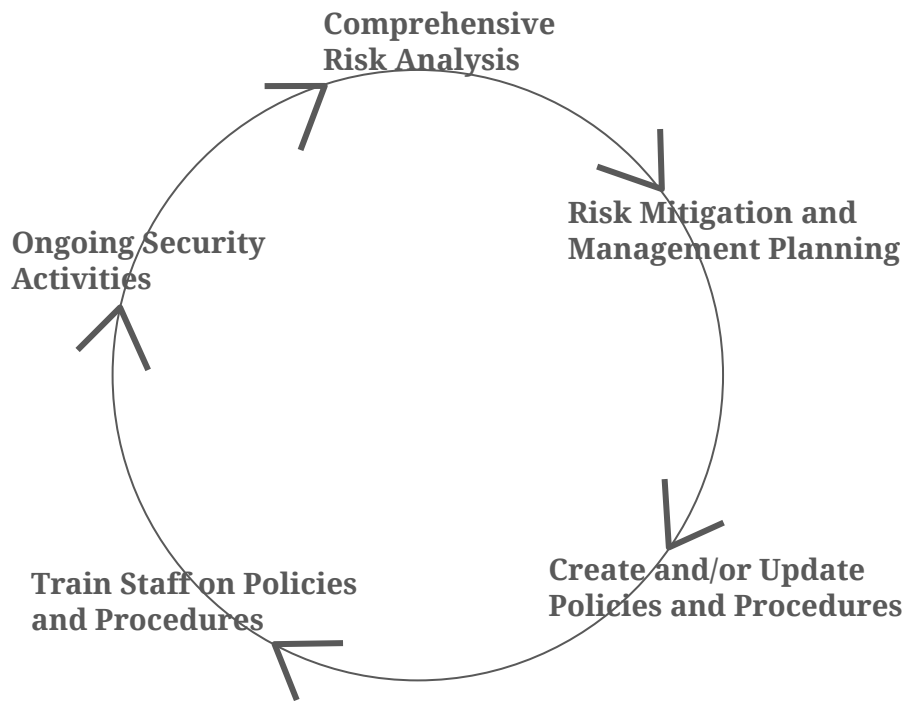


Why The Cycle of Security Activities?



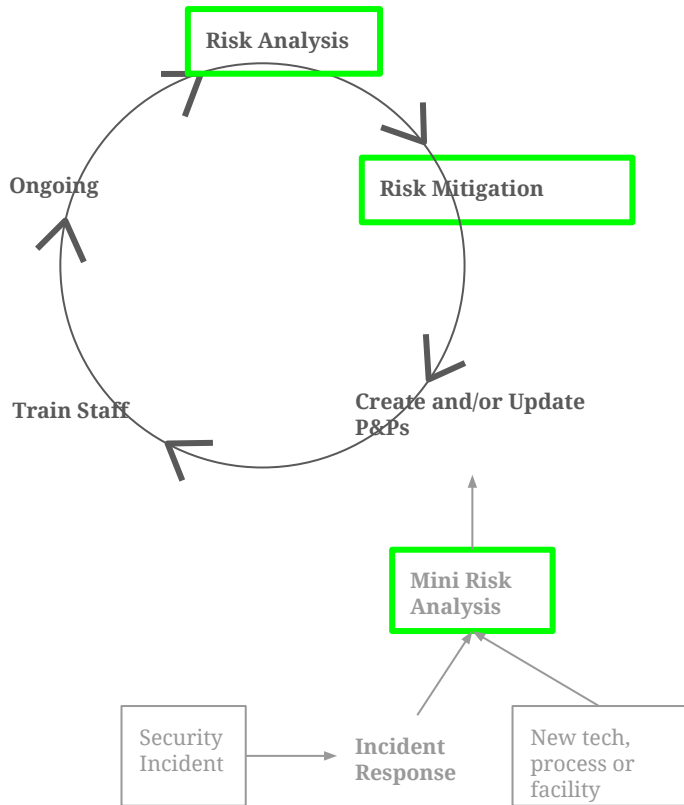
- The cycle diagram is a distillation of HIPAA's Security standards into an ordered set of high-level steps.
- Your program's activities can flow through the diagram's steps over time, and you can generally trust it to keep you on-track with maintaining compliance needs.
- In addition to distilling the steps for compliance, it also describes an effective, evidence-based security risk management program for small-to-medium organizations. (Here, "medium" often means, "smaller than a hospital system.")
- This model is harder to share with the staff than "the circle" is. It is most useful for leadership who are trying to conceptualize the direction of their risk management program.

Where Does The Cycle Start From?



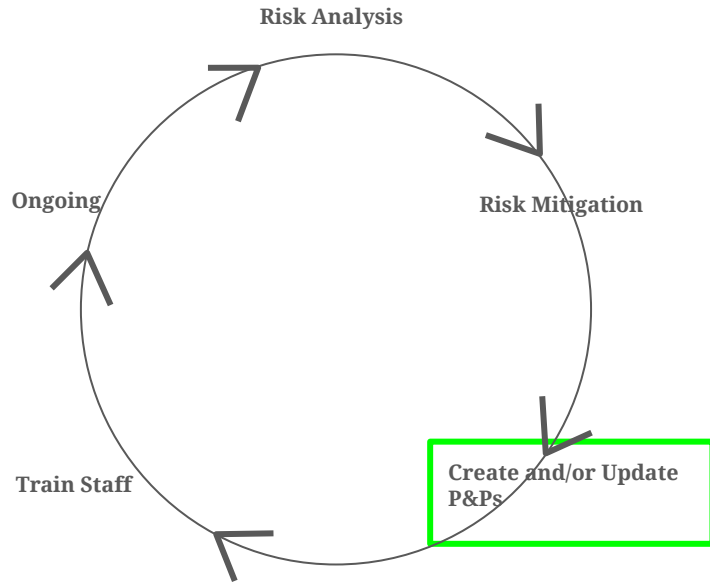
- Because all the other steps are informed by the risk analysis, the basic concept has us starting with the **Comprehensive Risk Analysis** step and then working from there. (*HIPAA Reading Unit 2*)
- However, many practices first **Create Policies and Procedures** related to their most common activities -- such as device security, communications security (e.g. email and texting), and Bring Your Own Device (BYOD). They then move on to the **Comprehensive Risk Analysis** after they **Train Staff on those P&Ps** and then **Ongoing Security Activities** related to the P&Ps are humming along.

The Cycle: Risk Analysis and Mitigation



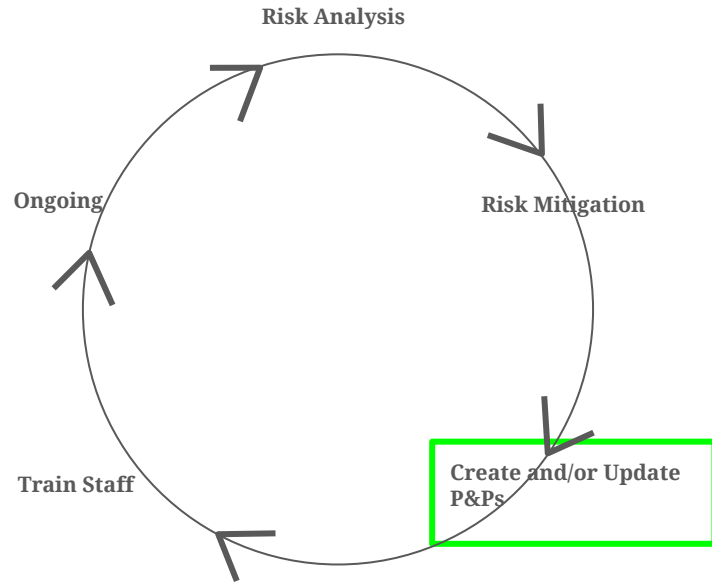
- **Comprehensive Risk Analysis:** usually do it about annually. If very little is changing in the practice, you might opt to skip it some years. After the first time, subsequent analyses will usually go much faster.
- A formal **Risk Mitigation and Risk Management Planning** process should follow each comprehensive risk analysis. That is where you take a comprehensive, holistic look at how the practice manages and mitigates the risks identified in the risk analysis.
- Do a **Mini Risk Analysis** when anything changes or when a significant problem is discovered -- such as following a security **Incident Response**.
 - Mini risk analysis is where you perform a risk analysis whose scope is only the particular assets or facilities that are impacted by the change or incident.

The Cycle: Policies and Procedures



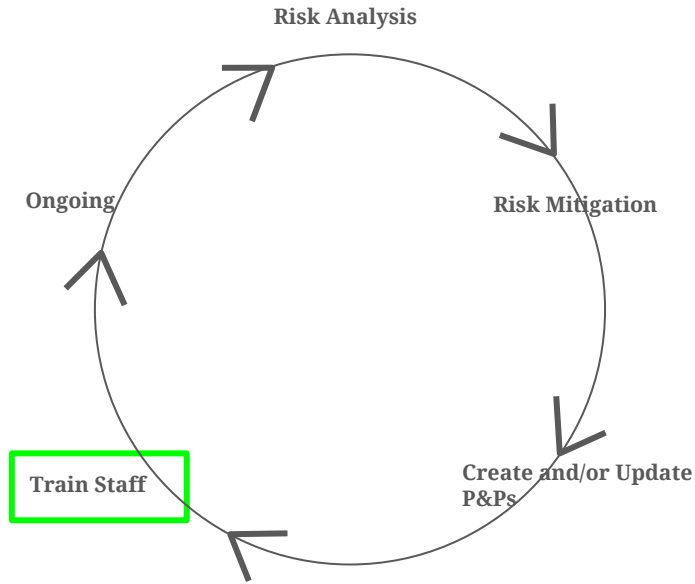
- After developing your strategy for risk management and mitigation, or when you simply need to get some structure into place for the risk management program, **Create and/or Update Security Policies and Procedures**.
 - These are internal policies for the staff. They are not for clients. The staff should be able to access them when needed.
 - These are *written documents*. They are for the staff, but they are also documentation of compliance with HIPAA.
 - Once a policy is updated or retired, retain the old version in your archives for at least 6 years, as required by HIPAA.

The Cycle: Policies and Procedures, Cont.



- Address all of HIPAA's Security standards -- make sure none of them gets missed.
- Make sure policies are not vague and do not imply or indicate that compliance is optional (except where it is, of course.)
- In addition to clearly defining the rules that staff must follow, provide specific guidance and structure for staff to behave securely, perform all regular security tasks, and stay on the same page with leadership and with each other.
- Policies and procedures can definitely be based on templates, but need to be reflective of the results of risk analyses. Their contents should not be developed outside the context of your practice and its needs.
 - You can work from templates such as the ones provided with Person Centered Tech's group practice services.

The Cycle: Train Staff



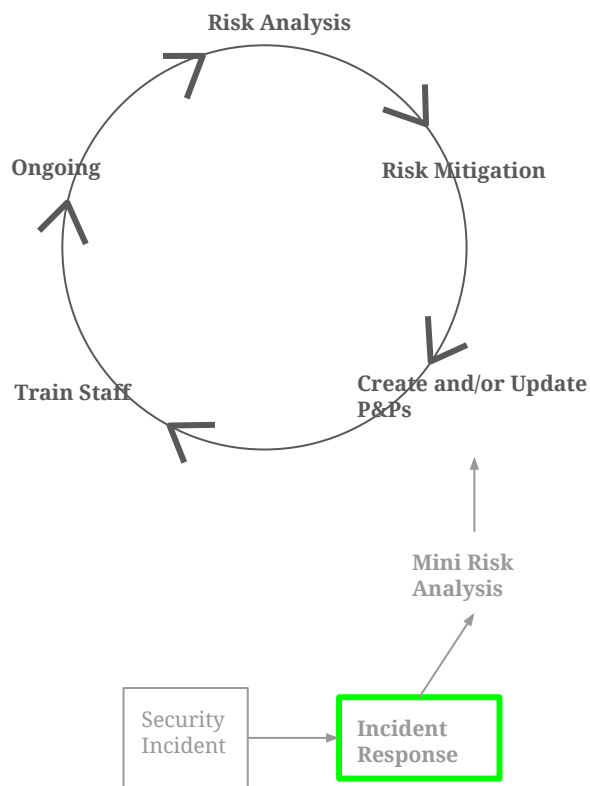
- When there are new policies, when you identify a problem that needs to be addressed, or just when you need to do something to keep the risk management program on everyone's mental radar, **Train Staff on Policies and Procedures** (also on security concepts needed to comply P&Ps, e.g. how to avoid phishing scams.)
- Training usually falls into two types:
 - *Formal training.* This can be events on-site, live webinars, self-study courses, assigned readings, interviews, or whatever accomplishes the task of educating the team.
 - *Security reminders.* HIPAA' Security standards require that reminders be part of the training program. These can be notices posted in staff-only areas, brief announcements before staff meetings, weekly update emails, or whatever you like. The idea is to emphasize important security ideas and/or to gradually teach the staff about bigger security concepts.

The Cycle: Perform Activities, Keep Logs



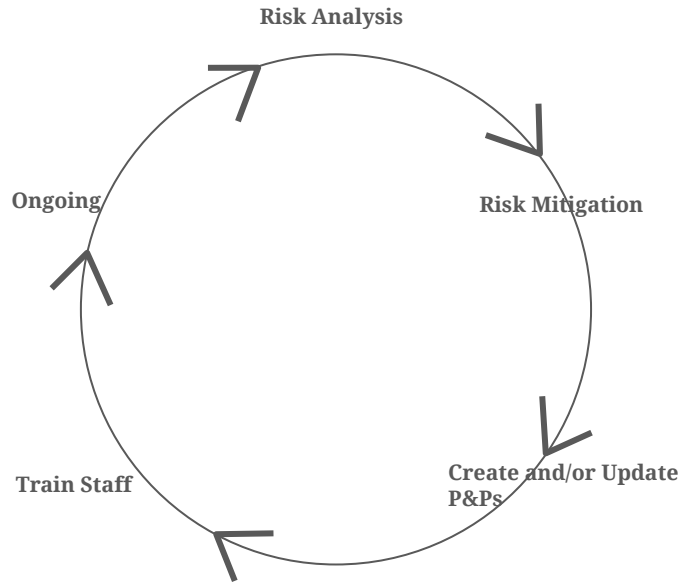
- The P&Ps will define several regular and irregular security tasks that are to be done. The exact tasks you need will depend on how your practice runs things. They include things like:
 - Perform backups
 - Analyze access logs
 - Check locks at the end of the day
 - Onboard staff members
 - Offboard staff members
 - And much more!
- Keep catalogs of assets and personnel. Log all security activities. Keep catalogs and logs for 6 years.

The Cycle: Incident Response



- When you or anyone else discovers a sign that a security breach might have occurred, you need to initiate a **Security Incident Response** process.
- Make sure staff know that reporting a suspected incident is not the same as reporting a confirmed breach. You need them to help you identify problems -- and a few false positives are much better than missed positives.
- Security incident response can have several stages to it, especially if you end up discovering an actual breach which requires notification. The process is very much the SO's domain and you will need to use your leadership skills to complete it. (*HIPAACore Module 5*)
- Many incident response processes reveal a security issue that needs to be addressed. That is why you should strongly consider a mini risk analysis and possible updates to P&Ps following each confirmed incident.

The Cycle: Tips to Make It Work, *P&Ps* & Training



- Make sure your P&Ps are actually effective at reducing the security risks facing the practice.
- Train staff as often as needed to ensure they can handle known security risks that might come their way.
 - E.g. at the time of recording, email phishing scams were on the rise. In such an environment, a practice's SO might give a special presentation or send out special materials about avoiding falling prey to email phishing scams.

The Cycle: Tips to Make It Work, *Culture & Support*



- Develop and foster a supportive security culture.
- Support the staff when they have technical needs.
- Be collaborative with staff members and patient when they need to understand why they're being required to make changes or do things they may not like.
- Make sure everyone knows the stakes being addressed by the program.