How to Create and Use HIPAA Security Policies and Procedures

Developed by Roy Huggins, LPC NCC
Presented by Roy Huggins, LPC NCC; Liath Dalton; and Nicole Kramer, MBA

Presented March 29th, 2018

Prologue

This is a CE session of Office Hours. That means it will be structured as a series of questions answered by the presenters. Office Hours is a 4 times/mo service provided to Person Centered Tech's members.

The Questions

Photo by Aaron Burden on Unsplash

Q1: What are HIPAA security policies and procedures and why do I need them?

A Documented Set of Security Plans

- "Documentation or it didn't happen"
  - All security practices are documented in P&P.
  - Actual security activities also need to be documented via activity logs.
- No specific way they must be done, but they do need to be thorough
- Here is the list of P&P document titles we created for our members who have a single clinician but one or more people who help in the practice:
  - Bring Your Own Device Policy, Contingency Policy, Data Backup Policy, Device and Document Transport and Storage Policy, Device and Electronic Media Disposal Policy, Device Security Policy, Office Security Policy, Passwords and Other Digital Authentication Policy, Risk Management Policy, Security Incident Response and Breach Notification Policy, Technology and Services Selection Policy, Workforce Management Policy… ***<u>the contingency plan</u>***

It's Required By HIPAA's Security Rule

> *"A covered entity must adopt reasonable and appropriate policies and procedures to comply with the provisions of the Security Rule. A covered entity must maintain, until six years after the later of the date of their creation or last effective date, written security policies and procedures and written records of required actions, activities or assessments."*
> *45 C.F.R. § 164.316.*

"...to comply with the provisions of the Security Rule."

- The evidence that one is compliant or not lies heavily in policies and procedures.
- Policies and procedures need to be written so as to ensure that all the HIPAA Security standards and provisions are covered somehow.
  - Let's see those standards: https://rusecure.rutgers.edu/hipaa-regulation-rbhs/6-hipaa-security-standards-matrix

When Will These Come Up?

- When people who work with/for your practice need to know how things work
- When you're trying to remember how things work
- Investigations/audits

Photo by Nathan Riley on Unsplash

Q2: How and when do I create or update my policies and procedures?

From Risk Analysis to Risk Mitigation to P&P

- While P&P need to address all of HIPAA's standards, they should reflect the needs and priorities identified in the risk analysis process. *They should reflect what the practice needs as well as what HIPAA requires.*
- The risk mitigation plan (which is built from the risk analysis) will generally provide guidance on which P&P, or portions thereof, need to be implemented earliest.

P&P Update When the Practice Does

- Following the annual risk analysis process
- When a big change is made in the office
- When a big change is made in tech
- When you go from solo to having helpers to, perhaps, a group practice!
    - The more people involved in your practice, the more vital P&P become. They can also get more complex.
    - Let's see an example of some P&P language for a solo practice vs. a group practice:

From our solo practice "Device Security Policy"

> *All electronic protected health information that is stored on computing devices or electronic media must be encrypted. Must be full-disk or full-device encryption.*

From our group practice "Computing Devices and Electronic Media Technical Security Policy"

> ***Encryption Policy***
> *All electronic protected health information that is stored on computing devices or electronic media must be encrypted. Where applicable, computing devices must employ full-disk or full-device encryption, which is abbreviated as "FDE." The Security Officer may use their discretion to decide what encryption solution is appropriate for each device and piece of media so long as FDE or its equivalent is accomplished.*

"...and written records of required actions, activities or assessments."

- Similar to P&P, a practice needs a way to log the various security assessments and activities that occur over the course of practice.
    - Performing backups

  - Changing passwords
  - Updating operating system software
  - Doing a HIPAA training
  - Etc.

Photo by Crew on Unsplash

Q3: What tools are available to help author security policies and procedures?

DIY

There is no specific reason you cannot develop your own P&P.

Challenges include:

- Sufficient time to complete them
- Sufficient expertise to make them thorough and use appropriate best practices

Advantages include:

- Your P&P can completely reflect your own practice culture
- You become very familiar with your P&P

Available HIPAA-Focused Risk Tools That Include P&P Templates

Links to tools are in the Resources section:

- HIPAACOW tool *[free to all]*
- NASW tool *[included for NASW members]*
- Person Centered Tech tools *[included for PCT members]*

Person Centered Tech supports members using *any* risk analysis tool. Members are not required to use anything we create in order to get support.

Photo by Krista Mangulsone on Unsplash

Q4: What do I do with my policies and procedures?

Training

- Workforce, both temporary and permanent, need some kind of training on the P&P related to their roles.
- Many workplace “HIPAA trainings” are, in fact, mostly trainings on the organization’s P&P.

“A covered entity must maintain, until six years after the later of the date of their creation or last effective date, written security policies and procedures…”

- Compliance documentation, in general, must be kept for at least six years.
- All P&P documents should have the following pieces of information:
    - A version number. It’s fine to simply number documents like 1,2,3,...
    - An effective date. This is the date in which the document first goes into effect.
- When you make a significant change to a P&P document, you should increment the version number and put the old version in storage to be held for at least six years.

Photo by Álvaro Niño on Unsplash