Performing HIPAA-Compliant Risk Analysis: A Guided How-To for Mental Health Professionals

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

Presented January 25th, 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.

Extra special thanks to Clinton Campbell, LMHCA CISSP for his assistance and validation in developing our risk analysis model.

The Questions

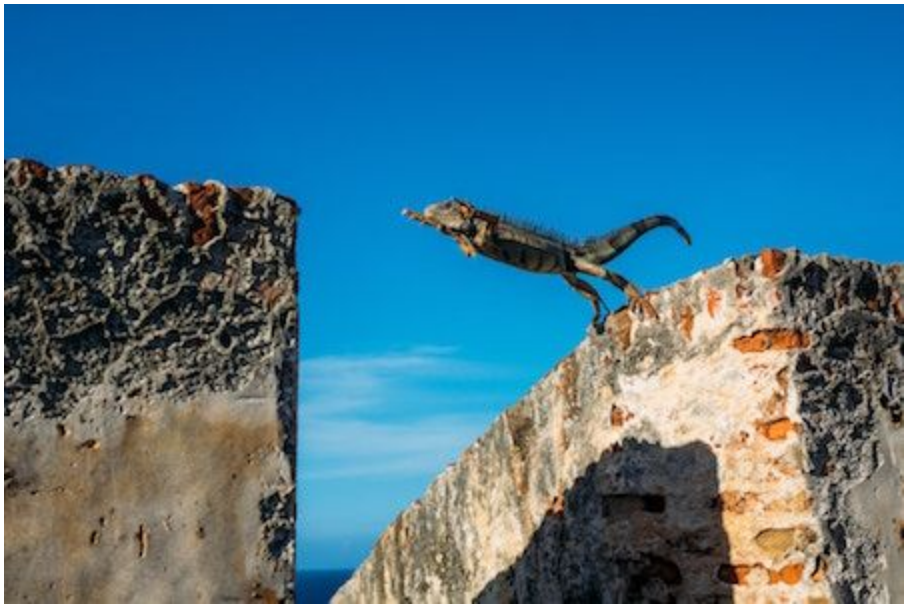


Photo by Denny Luan on Unsplash

Q1: What is Risk Analysis and Why Should I Care?

It's Required By HIPAA's Security Rule

> *"Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity."*
> *45 CFR § 164.308(a)(1)(ii)(A)*

Two vital points:

1. HIPAA's Security Rule only covers electronic information, so HIPAA only requires your risk analysis to cover electronic information. For ethical and practical reasons, however, we recommend you include all information and assets.
2. The only definition of risk analysis included in the law is that it be "accurate and thorough" and that it covers potential risks and vulnerabilities to "confidentiality, integrity, and availability" of ePHI.

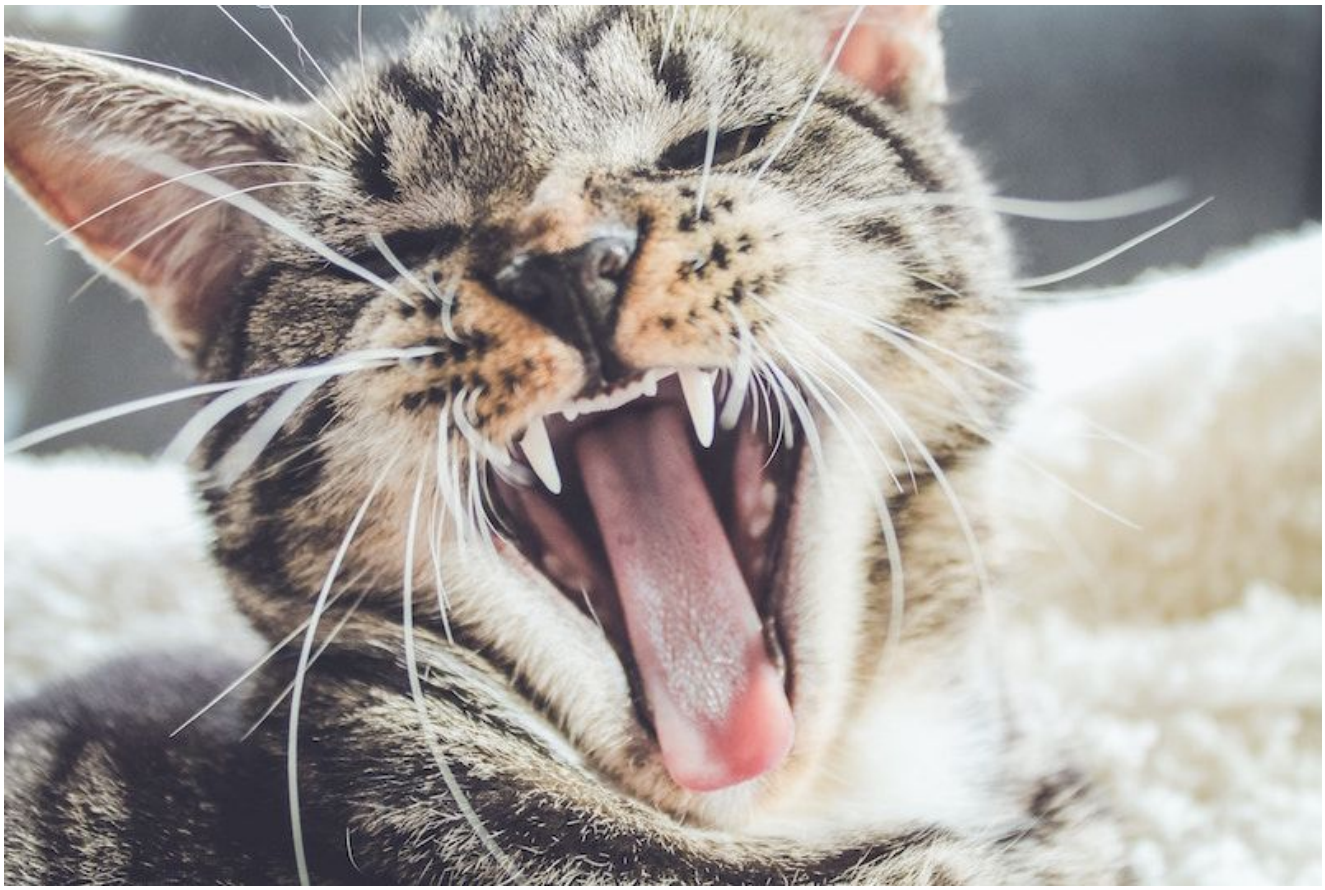
It's a Best Practice for Protecting You and Your Clients

Can you tell me, off the top of your head, definitive answers to these questions?

1. What is the physical location of all the emails you've exchanged with clients? I.e. what assets do you need to protect in order to protect your emails? (There may be more than 1.)
2. How would your client records would be impacted if you had an office fire?
3. Is the way you exchange texts or emails with clients the most secure method that is reasonable for you to use? Is there anything that would work better for you and your clients?

Risk analysis involves:

- A regularly repeated process (about yearly) where one formally reviews one's practice for risks and vulnerabilities.
- An ongoing process where one discovers new risks and vulnerabilities and takes steps to manage them. ***We have a good story about how ongoing risk analysis happens.***



Yaw-- I mean rawr!

(Photo by Erik-Jan Leusink on Unsplash)

Q2: How and When Do I Perform a Risk Analysis?

Process Summary According to CMS

The Center for Medicare and Medicaid Studies (CMS) wrote a guidance document for small health care entities in 2005 and 2007. The National Institutes for Standards and Technology (NIST) have more generic risk analysis guidance meant for all industries, and the CMS guide is a distillation and simplification of NIST's older guidance documents. We think the CMS guide is still relevant, even when compared against NIST's guidance updates that were released after 2007.

The CMS guidance process essentially comes down to these kinds of steps:

- **Assign responsibilities.** For most practices, that means designating someone as the Security Officer. That person will be in charge of the risk analysis process and also all other security processes. In solo practices, you get to be your own Security Officer. Congratulations! (Person Centered Tech will help you, of course.)
- **Document "assets."** Gather a big list of the practice's assets (includes people!) and PHI. Figure out how the two interact (e.g. which assets handle which PHI?)
- **Find threats and vulnerabilities.** Make a list of *reasonably anticipated* threats and examine how each one interacts with the vulnerabilities in your assets.
- **Rank risks.** Make a ranked list of risks based on the *reasonably anticipated* interactions between those threats and asset vulnerabilities. The ranking can be a simple rubric of high, medium, and low risks. NIST gives us some guidance on what "high, medium, and low" means, which we will discuss in the next question.
- **Make a plan**. Make a plan for mitigating the risks, starting with the highest ones and working your way down.

Timing

- The best practice is to repeat the risk analysis process every year.
- Perform a "mini risk analysis" when you make changes to your practice's tech, change offices, or other changes that impact the risk picture.
- Risk analysis is also ongoing -- just like assessment of clients' psychological state is always ongoing. The HIPAA Security Rule's standards define some measures to take that assist in keeping the risk analysis going.

Photo by Bing Han on Unsplash

Now let’s get inside the process!

Q3: How Does the Risk Analysis Process Go?

Risk-Based Analysis

There are a number of different paradigms for risk analysis. One that is commonly found is the "controls-based" paradigm.

"Controls-based" essentially means going through the big list of HIPAA Security standards, seeing if you've complied with them, and ranking risks based on how well you have or haven't complied. It's a rather abstract process, and we think it's difficult to use for people other than security professionals.

"Risk-based" means using one or more ways of anticipating potential risks to the practice and ranking those risks based on how likely and impactful they are weighed against how well the practice is currently protected from them. It is a more concrete method, and is likely easier for therapists and their helpers to do. It does require more knowledge of the threats and vulnerabilities we face, though, so it's a good idea to use a tool that was developed by experts.

Available HIPAA-Focused Risk Analysis Tools

Links to tools are in the Resources section:

- HIPAACOW tool *[free to all]*: Controls-based portion and risk-based (specifically threat-focused) portion.
- NASW tool *[included for NASW members]*: Formatted according to a control-basis, but assessment is done using risk-focused questions.
- Federal Health IT tool *[free to all]*: Purely controls-based.
- Person Centered Tech tools *[included for PCT members]*: heavily risk-based.

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

The Process as Curated by Person Centered Tech

The following steps (in bold) are quoted from the 2005-2007 CMS document's "Example Risk Analysis Steps." Comments between the steps are guidance from Person Centered Tech:

1) Identify the scope of the analysis.

Exactly what are you going to analyze? HIPAA would require that you analyze everything and every person in your practice that touches *electronic* protected health information. We recommend, for ethical and practical reasons, that you expand the scope to include all protected health information in any form.

It would also be wise to set a timeframe for your analysis. Generally, most practices will want to consider "risks that are reasonably anticipated to occur from XX/XX/XXXX to YY/YY/YYYY." It usually works for those dates to cover 1 year.

This is also a good step in which to *assign responsibility*, generally meaning you designate someone as the Security Officer.

2) Gather data.

→ Get a thorough inventory of all the "assets" in the practice. That includes people, computers, online accounts, etc. For devices, office equipment, and other material goods that touch information: make a note of who is *responsible* for each asset and who *owns* each asset.

→ Next, get a thorough inventory of all the information your practice "creates, receives, maintains, and transmits."

→ Tie the information to the assets. In other words, give yourself a picture of which assets handle which information.

→ Give each asset a "criticality rating," which is a rating of how vital the asset is to your ability to *keep operating and accessing your information.* Note that this is different from a risk rating. For criticality, what you're trying to do is get a picture of which assets you need in order to be able to access info or keep the practice running. These ratings will be essential when you come up with a contingency and/or continuity plan.

→ The Feds also like for practices to have a "network diagram." That means a picture of where your electronic devices and information are relative to each other. A simple version of this could be to sketch out the location(s) where you do your work, and to note in the sketch where your non-mobile devices are. *Make sure to include all routers and WiFi gear and how they are or are not physically protected from tampering.*

3) Identify and document potential threats and vulnerabilities.

This is where we get into the different styles of risk analysis: controls-based, risk-based, combos of the two, etc.

There are many philosophies and styles for how to do this. The tools mentioned above all exemplify different examples.

The idea is to come up with things that can threaten your assets' abilities to keep information safe and/or available, and then pair those threats up with the ways in which your assets are vulnerable. At this point, it becomes apparent why expert-created tools, at the very least, are generally needed.

4) Assess current security measures.

For all those threat-vulnerability pairings from step 3, make a survey of the measures currently in place that reduce the likelihood of the threat acting on your asset(s); or that reduce the impact it can have on your asset(s.)

Measures can be a wide variety of things, from "full disk encryption" for computing devices to "password policies" to "sprinkler systems" and on and on.

5) Determine the likelihood of threat occurrence.

For each of those threats, rate the likelihood that the threat will be able to act on your asset(s) in question.

NIST guidance suggests rating likelihoods as 0.1, 0.5, or 1.0. The reason will become apparent in step 7, but know that these number correspond to a "low, medium, or high" rating scale.

6) Determine the potential impact of threat occurrence.

Now determine the *potential* (but still reasonably anticipated) potential impact of those threats on those assets. NIST recommends a scale of 10, 50, or 100. Once again, these correlate to a "low, medium, or high" scale.

7) Determine the level of risk.

For each of the risks assessed above, multiple the likelihood rating by the impact rating. This way, each risk ends up with a numeric rating from 1 - 100.

Note that this system accommodates your ability to contemplate risk impacts and preventive measures separately -- i.e. you can think about just how bad a threat could be and also think about how well you're preventing it in parallel. There's no need to go back and forth between the two thoughts. The rating system will take both issues into account.

When you've rated everything, sort your list of risks from highest risk score to lowest.

8) Identify security measures and finalize documentation.

This is where you make a plan for coming up with new security measures to reduce your risks to acceptable levels. That's outside the scope of this training, but we'll touch on it in the next question!

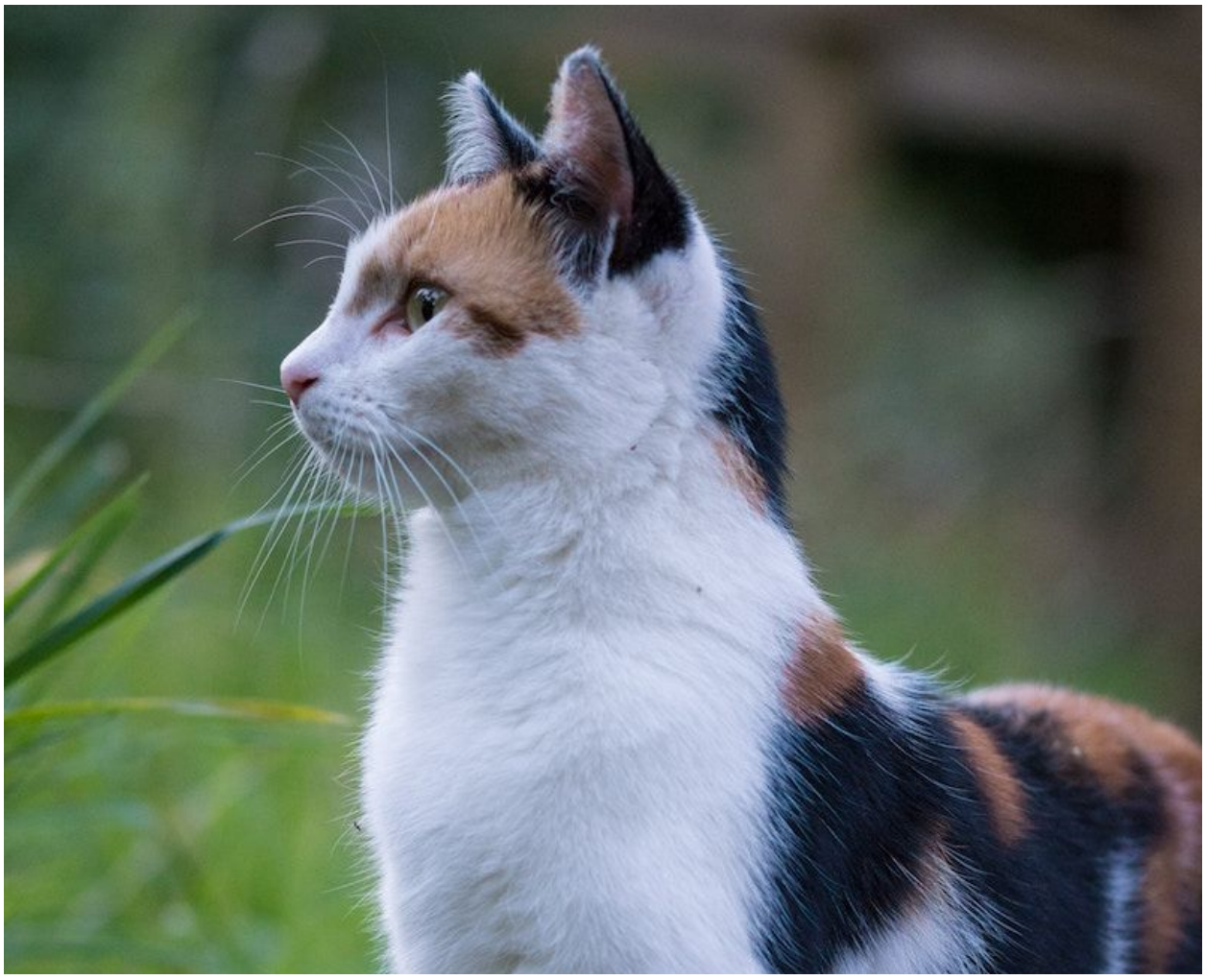


Photo by Uriel Soberanes on Unsplash

Ready for the last steps?

Q4: What Do I Do With the Results?

The details are outside the scope of this training, but here's the gist:

Risk Mitigation Planning

Make a plan for how you are going to reduce your risks. You generally prioritize the higher ones and work your down.

HIPAA does not expect you to mitigate everything at once -- quite the opposite!

Also, remember that you need to ensure that your chosen security measures include all the standards defined in the HIPAA Security Rule. This is where controls-based tools shine -- they help you ensure this throughout the process.

Note that the measures you come up with need to be documented in the form of policies and procedures…

Make Policies and Procedures

The Security Rule does require you to have a set of security policies and procedures that address all the risks you've identified and also cover all the Security Rule standards. The various tools provide varying degrees of help with this:

- HIPAACOW tool *[free to all]*: Template policies and/or guidance for nearly HIPAA Security standards. Written very technically and how often abstractly, however.
- NASW tool *[included for NASW members]*: Several template policies, but the set appears to be incomplete.
- Federal Health IT tool *[free to all]*: No template policies.
- Person Centered Tech tools *[included for PCT members]*: Currently includes some template policies written specifically for mental health practices. The full set of templates is in ongoing development at this time.

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

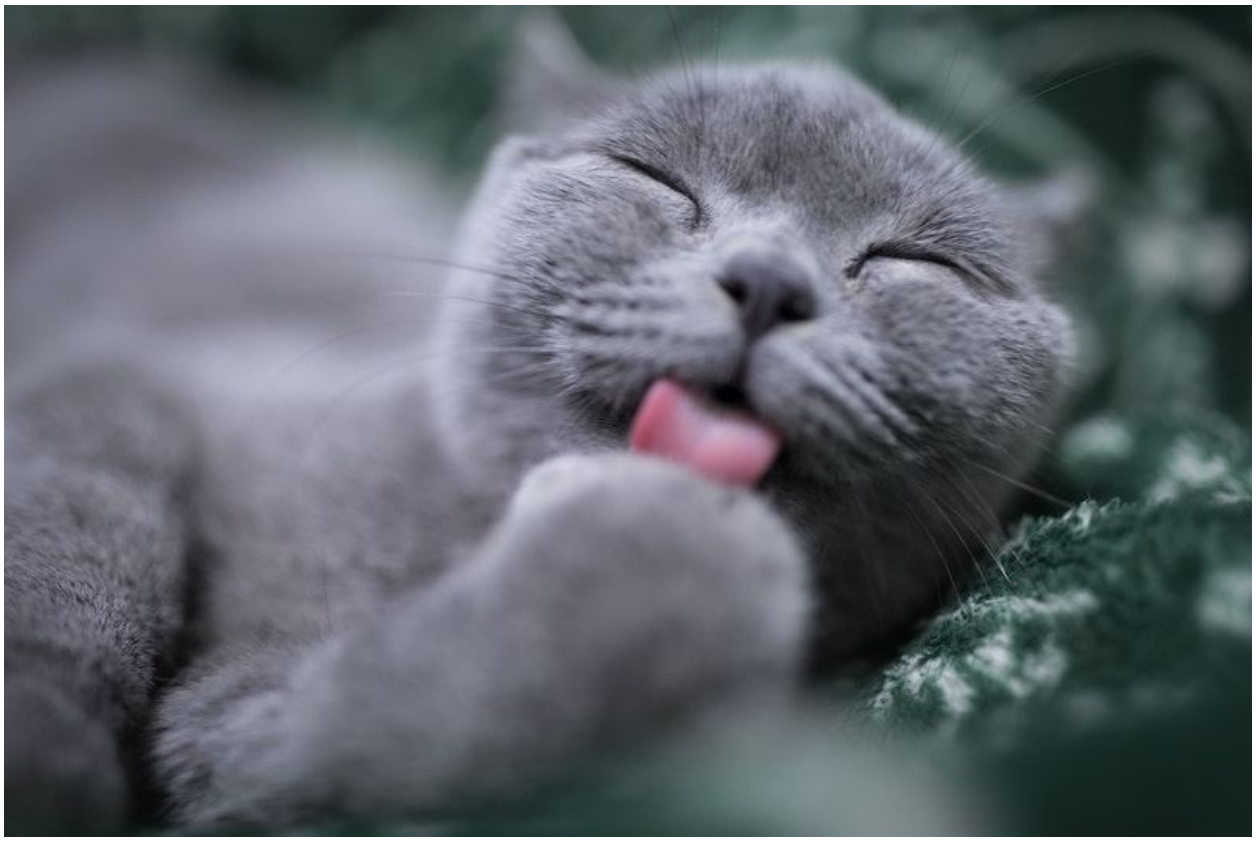


Photo by Eric Han on Unsplash

Take a breather!