HIPAA SECURITY CHECKLIST

OVERVIEW

The HIPAA Security Rule, may not be the most comprehensive, and may not guarantee security, but it's great because it tells organizations to think through how they protect information in terms of risk. And while the Office for Civil Rights at the Department of Health and Human Services provides guidance for what they mean by a risk assessment, they are reticent to explicitly provide a step-by-step how-to for conducting a risk assessment. You can find HALOCK's guidance for risk analysis in presentation format and as documented guidance in The Best Guide to the HIPAA Security Rule You'll Ever Read.

ABOUT THIS CHECKLIST

For the process of implementing and maintaining a HIPAA Security and Compliance Program over time it's helpful to have a checklist. Keep in mind that the HIPAA Security Rule requires continuing oversight for security, therefore you can approach your HIPAA Security and Compliance program the following way:

STEP	ACTION	COMPLETED?
GET ACQUAINTED.	Watch HALOCK's "Surviving the HIPAA Security Rule" presentation to understand the objectives of the HIPAA Security Rule, and what compliance actually means.	Presentation watched? ☐ Yes ☐ No
UNDERSTAND.	Print, read, and share "The Best Guide to the HIPAA Security Rule" with your coworkers, like risk managers, compliance managers, privacy managers and Counsel to ensure everyone has the same understanding of the detailed requirements of the HIPAA Security Rule specifications. The Guide will help you think through how much of each specification you need to apply.	Guide printed, read, and shared? ☐ Yes ☐ No
IDENTIFY YOUR ASSETS.	Information assets include records, facilities, systems, applications and people. Develop a list of these information assets and determine who in your organization is responsible for those assets.	Lists developed? ☐ Yes ☐ No
MAKE YOUR RISK REGISTER.	Follow the guidance in the presentation and document above to assemble a spreadsheet that itemizes the Security Rule specifications, and models threats against your assets that store, secure, or transmit PHI.	Risk register developed? ☐ Yes ☐ No
DEFINE REASONABLE.	What impact and likelihood is acceptable to your organization? How do you define that? How do you know when analyzing a specific risk that the risk is above or below the level of acceptable risk?	Definition for reasonable? ☐ Yes ☐ No
ANALYZE RISK.	When considering each Security Rule specification, think through how your information assets are protected with that specification. Think through the information security threats that can foreseeably compromise the assets in a way that causes harm to others or your organization, and estimate the 'impact' and 'likelihood' of that threat. *TIP: Keep in mind that the HIPAA Security Rule is vague, and not comprehensive, as far as security standards go. Consult documents such as NIST 800-53 to identify security controls that should be considered on top of the Security Rule specifications.*	Impact / Likelihood estimated for threats? ☐ Yes ☐ No

STEP	ACTION	COMPLETED?
DEVELOP A PLAN.	For risks that are above your acceptable level of risk, consider safeguards that would create an impact and likelihood that is equal to or less than your acceptable level of risk. *NOTE: Remember that an impact may hurt your mission, your objectives, or your obligations to not harm others.*	Safeguards explored? ☐ Yes ☐ No
IMPLEMENT SAFEGUARDS.	It should now be evident whether the safeguards you intend to implement are reasonable. Start implementing. *NOTE: Implementation is not solely a technician's job. Any person who is responsible for an information asset must own the risk of that asset, and must own – to some degree – the successful implementation of its safeguards.* *If a control or process is not getting implemented on time, the asset's owner needs to know, and needs to make provisions for putting in place some safeguard that reduces risk to an acceptable level.*	Safeguards implemented? ☐ Yes ☐ No
TEST SAFEGUARDS.	Determine whether your newly implemented safeguards are working well. NOTE: Internal audits and security testing can be very useful here. Check to see if people are following processes. If not, why not? They may have a very good reason for not complying. Are safeguards too burdensome? Do they conflict with your mission? If so, these are by definition "unreasonable" controls. FOR EXAMPLE… Maybe some controls are in place, but not operating, or your personnel are overwhelmed by having to manage new technologies. These are by definition "unreasonable" controls. Either consult with specialists who can help you make these tools and processes more reasonable, or consider new safeguards. (Or increase your budget to support safeguards).	Safeguards evaluated? ☐ Yes ☐ No
EMBRACE KAIZEN.	Kaizen is the Japanese practice of continuous improvement. Optimize your safeguards as part of your business as usual process. Managing HIPAA is not a one-time event. It's a continual and evolving process. Your safeguards need to keep up with the threats to your data. *NOTE: The HIPAA Security Rule, and any other regulation we can think of, requires that you know when your safeguards are not working so you know to fix them. This means that your team needs to feel comfortable pointing out, and even seeking weaknesses and reporting them up.*	Continuous improvement in place? ☐ Yes ☐ No
CREATE A RISK-FOCUSED CULTURE.	Develop and foster a culture where staff are actively examining safeguards and are comfortable pointing out when things are going wrong. Encourage employees to take ownership of those weaknesses. *NOTE: Creating a risk-focused culture is perhaps the biggest challenge in information security, but it's critical to fix.*	Risk-focused culture implemented? ☐ Yes ☐ No

Was this helpful?
We hope you found these materials helpful and a great place to start on your HIPAA compliance program. Keep in mind that OCR wants to see a conscientious effort toward identifying risks and resolving them with a plan. Having a basic checklist may get you well on your way.