Below we have provided a beginning checklist, a starter kit, if you will, to get you on your way to full HIPAA compliance and peace of mind. Remember that as stated in the previous article about **getting started with HIPAA compliance**, this will help you to develop a framework around which to begin remediation.

Compliance Assessments and Audits

Every compliance initiative begins here. There can be no improvement without measurement (assessment) first. OCR has provided a list of essential audits and assessments to establish a baseline from which to begin compliance remediation and continued maintenance.

- Security Risk Assessment
- Privacy Assessment
- HITECH Subtitle D Audit
- Asset and Device Audit
- Physical Site Audit
- Security Standards Audit

Staff Training

With end users being the single biggest attack surface in the office, documentation of continuous training is not only one of the best ways to show and prove due diligence in maintaining compliance, but also the last line of defense of your organization from malicious attacks.

- Have all staff completed annual HIPAA training, and are you able to provide documentation of successful completion?
- Are all users receiving ongoing security awareness training, and can you provide documentation to prove it?
- Have you designated a staff member as your HIPAA Compliance Officer?

Periodic Risk Assessment

Your organization is ever changing. With each new application, update, hiring, employee exit or similar change, a new vulnerability or compliance violation is potentially introduced. Prevent gradual non- compliance creep by doing the following on a predetermined schedule.

- How often do you evaluate technical controls such as password policy, encryption, and antivirus to ensure that network vulnerabilities do not potentially expose PHI?
- How often do you assess administrative controls to ensure that policies, procedures and training, promote and enforce adherence to compliance regulations?

Identity Management and Access Controls

Identity and Access Management (IAM) is one of the cornerstones of PHI protection, and must be implemented to ensure Access, Authorization and Accounting (AAA) is enforced, monitored,

and documented.

- Have you assigned unique usernames (identities) to all individual who access PHI?
- Have you implemented a password complexity policy and a threshold at which passwords must be changed?
- Have you implemented a "least privilege" policy to ensure that staff members who do need to view or use data containing PHI do not have access to it?
- Have you developed exit policies to ensure that PHI is protected during the termination process?
- Does your system automatically logout a user after their session has been inactive for a set period of time?
- Is all this documented?

Monitoring, Logging, Auditing

- Have you implemented controls and procedures to protect against malicious or accidental data loss?
- Have you implemented a logging system to help you to track access to, modification, and movement of PHI? Are you effectively parsing these logs to continuously maintain and improve your security and compliance posture?
- Can you effectively enforce nonrepudiation through your current logging solution?

PHI Archival and Safe Disposal

Required data containing PHI must be stored for a minimum of 6 years, although some states may require more. This data must be safely disposed of when it is no longer needed. HIPAA outlines the requirements for storage and disposal.

- Are you archiving and backing up required data to long-term storage? Are you receiving and storing periodic reports of completed backups and retrieval exercises?
- Do you have policies and procedures in place for rendering data unreadable or indecipherable in the event it is compromised (is it protected)?
- Do you have policies in place for permanently erasing or destroying PHI when it is no longer required? Are you able to provide receipts of its disposal date and method?

Incident Response Plan

This is where the HIPAA Notification Rules are satisfied, among many other requirements. In the event of an incident, the breach must be contained, damage must be assessed, vulnerabilities must be addressed, logs must be made available for forensics investigations, proper entities must be notified, and a laundry list of other things must happen, all in the middle of a firestorm. This explains why a well-designed and rehearsed plan to address it all is necessary.

- Do you have an ordered contact list of all required entities, such as patients, The U.S. Health and Human Services Office for Civil Rights (OCR), local media, and local law enforcement to notify in the event of a breach?
- Do you have an immediate response plan to stop and isolate the attack, discover the source and cause, mitigate damage, and recover as quickly as possible?
- Do you have a procedure by which employees may anonymously report potential violations or practices?

That's a lot of questions to answer, but in the event of incident or audit, you must have answers for all of them. An explanation of exactly why is given **here**. And there is so much more than just this list.
Remember, this is only to help you to develop a framework from which to begin assessment and remediation toward compliance. Download a PDF of the Starter Kit here to get started. **Contact us** to get help answering these questions and taking the next steps toward full compliance.

About the Author

Mundell Phillips is the CEO and Principal Security Engineer with Nutech Solutions. Prior to Nutech, his work experiences include over 15 years technical and managerial roles in the private and public information technology and cybersecurity sectors. Mundell has led the design and implementation of several disaster recovery, security and compliance remediation projects for the proverbial alphabet soup of Government agencies (DOD, VA, DOJ, DOT, etc.). He has now committed his knowledge and experience to tailoring those same solutions to local ambulatory services providers and others under regulatory compliance mandates, with special focus on those serving our underserved communities in the greater DMV.