Ten Secrets to Surviving a HIPAA Audit or Investigation

A HIPAA program must be specific and customized to your office. No cookie-cutters allowed!

It also has to meet the test of being active and dynamic (can't just sit on a shelf month after month).

There are about 12 reviews, evaluations, and/or audits that have to be completed every single year [or more often] or your program is not active and dynamic and you will be in line for fines!

HIPAA law is enforced by the Office of Civil Rights (OCR) in conjunction with the Department of Justice.

Let's look at the secrets to surviving a HIPAA audit—but first, let me remind you that on numerous occasions, at the Washington DC Cybersecurity Symposium, the government has stated that YOU HAVE NO HIPAA PROGRAM AT ALL (no matter what else you think you have done to meet some part of HIPAA) IF YOU DO NOT HAVE A RISK ANALYSIS AND RECENT ISARs; therefore, while all of the following is critical, to meet government regulations, they are meaningless if you are missing a Risk Analysis and recent ISARs.

Here are the secrets to passing government scrutiny (with a bit of detail, like it might appear in the table of contents of a well-constructed HIPAA manual).

Secret #1:

Appoint a Compliance Officer!

a. They must have a Job Description - It is required that your compliance officer has a documented job description and they have officially accepted the position.
b. Notification of Officer Appointment/Posting - This must be correctly filled out with private information relative to your primary and secondary compliance officers, once you have decided how many you need and who they will be.
c. Filing a complaint – you must have the required documents (from OCR) available, on your premises during all hours that you treat patients and this MUST be issued to the patient in the event of a stated complaint or concern over mishandling of their private health information (PHI). It is critical to have this document in place, should you ever need it!

Secret #2:

Issue Notices of Patient Privacy Policy (NPPP) and create Business Associate Agreements (BAA)

a. 2013 Omnibus Rules, increased enforcement and fines relative to these two items.

b. You must have BAA's in place with every individual or entity that stores, transmits or has access to your patient private data (billing services, IT people, shredding companies, etc.) The government started random audits for these in 2018.
c. (NPPP). This document must be GIVEN to every new patient, per 2013 Omnibus Rules. It is critical and must include a signed acknowledgement from the patient that they received the document… this is one of new rules with increased enforcement and fines. This is being heavily enforced!

Secret #3:

Keep all HIPAA documents for 6 years… policies, procedures etc. must have a retirement date and be kept! This would include things such as your forms:

a. Consent to use PHI
b. Restricted Consent
c. Patient Authorization
    i. Revocation of Authorization
d. Approve Request to Copy
    i. Deny Request to Copy
e. Required Accounting Log – Per Patient
    i. This has nothing to do with the patient's balance… this is regarding a required accounting of everywhere you have sent the patient's private information out of your office… who it went to, what was included, why it went, etc.

Secret # 4:

Meet all training requirements:

a. Annual Required Staff In-Service Training - Privacy and Security Rules----There are certain topics you must cover and at the Cybersecurity Symposium in 2017 officials stated they thought a minimum of two per year should be done.
b. Have new employees sign Employee Confidentiality Statements
c. Issue MONTHLY security reminders to your workforce (per 2017 Cybersecurity symposium.

Secret #5:

Perform a yearly Physical Plant Audit

Secret #6:

Perform and update a Risk Analysis and ISAR's (Information System Activity Reviews)

a. Risk analysis is required to be audited at least once per year and must be updated every time you add or subtract an electronic device from use. It consists of five main components including a Gap Analysis and Mitigation Plan.
b. Information System Activity Reviews (ISARs), including audit logs, must be periodically performed and documented.

Secret #7:

Author all of the required Policies and Procedures for Security Rules

The following must have written policies and procedures. For most offices, this takes over 100 pages of documentation:

i. AUDIT SCHEDULE
ii. PRIVACY OFFICER / COMPLIANCE OFFICER
iii. PRODUCTION OF DOCUMENTS AND DATA
iv. RETENTION OF DOCUMENTS AND DATA
v. SANCTION POLICY
vi. CONFIDENTIALITY AGREEMENTS AND B.A. CONTRACTS
vii. SCOPE OF PROTECTION UNDER THE SECURITY RULES
viii. APPLICABLE STATUTES / REGULATIONS
ix. TEAM MEMBER/WORKFORCE POLICIES
x. PROHIBITED ACTIVITIES
xi. SECURITY MANAGEMENT PROCESS - RISK ANALYSIS
xii. EMERGENCY OPERATIONS PROCEDURE
xiii. EMERGENCY ACCESS
xiv. BUILDING SECURITY
xv. ELECTRONIC COMMUNICATION
xvi. INTERNET ACCESS
xvii. REPORTING SOFTWARE MALFUNCTIONS
xviii. TRANSFER OF FILES BETWEEN HOME AND WORK OR EMPLOYEE TO EMPLOYEE
xix. INTERNET CONSIDERATIONS
xx. DE-IDENTIFICATION / RE-IDENTIFICATION OF PERSONAL HEALTH INFORMATION (PHI)
xxi. USER LOGON AND IDS
xxii. ACCESS CONTROL
xxiii. DIAL-IN CONNECTIONS
xxiv. MALICIOUS CODE
xxv. ENCRYPTION
xxvi. TELECOMMUTING
xxvii. SPECIFIC PROTOCOLS AND DEVICES
xxviii. RETENTION / DESTRUCTION OF MEDICAL INFORMATION
xxix. DISPOSAL OF EXTERNAL MEDIA / HARDWARE
xxx. MANAGING CHANGE
xxxi. AUDIT CONTROLS
xxxii. BREACH NOTIFICATION PROCEDURES
xxxiii. CONFIDENTIALITY / SECURITY TEAM (CST)
xxxiv. CONTINGENCY PLAN
xxxv. SECURITY AWARENESS AND TRAINING
xxxvi. EMPLOYEE BACKGROUND CHECKS

Secret #8:

Have a Required Contingency Plan with Data Recovery and Emergency Mode Operations

The OCR has stated this written plan for data recovery and emergency mode operation will likely become the most important of all, over time, due to ransomware attacks, etc.

Secret #9:

Keep the Required Equipment Maintenance Log

You are required to have a log that records who and when anyone works on equipment that stores or transmits PHI.

Secret # 10:

Use Model Releases for Testimonial Use

Hopefully this quick overview of the most important secrets helps you understand the breadth of the HIPAA law and what you are required to do. We know it can be overwhelming to both initiate a program and then **KEEP IT CURRENT,** as required by law, but we stand by to assist you with several levels of services for installation and maintenance of your HIPAA program.

Please contact us at 214-437-7559 or ty.talcott@gmail.com or visit our website at www.drtythecomplianceguy.com