Automation Can Help Manage Complex Privacy and Information Security Compliance

By Judi Hofman, BCRT, CHPS, CHP, CHSS

WHEN THE DEPARTMENT of Health and Human Services' (HHS) Office for Civil Rights (OCR) starts to demand evidence of compliance months or years after a privacy or security event, do you ever feel like the evidence of your own investigation is inadequate? Does your evidence now look like something from "The Walking Dead," zombified with unrecognizable, decaying bits and pieces of evidence that can't be reassembled into a coherent defendable investigation? How do professionals overcome these issues and remain HIPAA compliant?

In order to reduce the risk of fines, penalties, and civil lawsuits, organizations should consistently retain and manage all records related to internal privacy and security investigations. Tracking of breach determination and corrective actions must be documented and retained in formats that illustrate consistency to external regulators such as OCR or other governmental oversight agencies. Because HIPAA was only minimally enforced prior to HITECH in 2009 there was little incentive to spur automation of investigation and breach determination processes, or any other HIPAA-based processes for that matter. But with ever increasing enforcement, applications automating privacy and security incident management have become available in the marketplace.

Documenting Privacy and Security Investigations

Currently, a majority of hospitals, clinics, and business associates utilize spreadsheets with manual entry to document the investigation, determination, and resolution of a breach incident. This is a laborious and time-consuming way to document and retrieve the information should a regulator agency come calling. It's also confusing and must rely upon reports developed by the privacy officer or staff who manages and documents an investigation, if any reporting exists at all.

As healthcare increasingly becomes more interconnected and larger organizations merge with smaller ones, the demands of accountability on privacy and security compliance becomes increasingly more important as outlined under information governance initiatives. Overall management of privacy and information security events under information governance help to assure leadership/organizational Board of Directors members that they have a compliant program in place.

The use of an automated tracking and trending tool has proven to be what is needed to help cut the time between initial investigation of an incident, breach determination resolution, and the subsequent six-year retention. HHS provides guidance within Section 164.316(b)(2)(i) that requires that HIPAA-related policies and procedures should be retained for six years as well as specific audit and logging under HIPAA Security Regulation 164.308(a)(5)(ii)(C) Logging, 164.312(b): Audit controls 164.308(a)(1)(ii)(D): Information system activity review. The Administrative Simplification Rule 45 CFR Parts 160, 162, and 164 require a covered entity retain required documentation for six years from the date of its creation or the date when it last was in effect, whichever is later. Combining the Administrative Simplification, Security Rule, and HITECH Breach Notification obligations, covered entities can take the six-year guideline and apply it to most documentation needs. Having an application or tool that contains data fields ready for population that meet documentation requirements mandated by the HIPAA and HITECH privacy and breach reporting rules can speed up and keep track of the entire lifecycle of an investigation.

It is imperative for accurate reporting to capture all the data elements necessary to perform breach determination and, if necessary, HIPAA and state reporting to the state attorney general, if required by state law. This entails dozens of data points and

multiple selection menu items.

A privacy and security incident investigation and reporting application should at least contain the following elements in order to meet HIPAA breach notification rules and the other HIPAA-required processes:

- Incident details including dates, persons involved, and general facts illustrating the "who, what, where, when, why" of the privacy/security incident. For example, captured information should include the nature and extent of the protected health information (PHI) involved, including the types of identifiers and the likelihood of re-identification; the unauthorized person who used the PHI or to whom the disclosure was made; whether the PHI actually was acquired or viewed; and the extent to which the risk to the PHI has been mitigated.
- Capture of all required OCR reportable data fields, with pre-populated selection menus.
- Task management to keep staff on track and on time.
- Ability to e-mail reminders and act upon responses.
- An assessment of whether the incident is an impermissible access, use, or disclosure and whether it is a violation of HIPAA and/or corporate policy.
- Assessment of whether the incident meets HIPAA breach exceptions outlined in 45 CFR 164.502. The first exception applies if the unintended recipient of the information would not reasonably have been able to retain the information (i.e., the information is recovered before it could have been seen). The other two exceptions apply to certain unintentional or inadvertent disclosures within a covered entity or business associate (i.e., an employee accidentally receives and opens an e-mail that was intended for a different employee or a physician sends a nurse the wrong patient's information) provided that the information is not further used or disclosed in an impermissible manner.
- An Omnibus four factor risk analysis—which analyzes the nature and extent of the PHI involved and likelihood of re-identification, who used the PHI or to whom the disclosure was made, whether the PHI was actually acquired or viewed, and the extent of risk that the PHI has been mitigated.
- State breach analysis (some privacy/security events may trigger reporting obligations under state data breach notification laws).
- Records of mitigation, remediation, and corrective actions.
- Timeframes logged and managed throughout the investigation and notification processes.
- Records of required notifications.
- All required reportable data elements in a single report for breach reporting to OCR or state agencies.
- Easy reporting of all elements of any single incident in case OCR requests an investigation or audit.
- Security incident management data elements based on National Institute of Standards and Technology guidelines.
- Clearly readable and highly sortable dashboards and reports.

While automating HIPAA processes, there are other procedures requiring workflows and timeframes which can be successfully automated. These include: amendments; restrictions; accounting of disclosures; other documentation, such as security risk assessments; and business associate oversight and the satisfactory assurance tracking.

There are "out of the box" solutions that have tools with basic configuration capabilities and self-service features. Customization of these may be limited and very time consuming to tweak to fit the needs of HIPAA documentation noted in this article.

Organizations may have already purchased tools that are not built specially for HIPAA (RSAM, IRIS, Origami Risk, EthicsPoint, etc.) that are used by risk management, compliance, and human resources departments, and have "tweaked" the database application to be used by privacy officers for HIPAA tracking. Most database tools and applications are not vetted as "compliant," but they may have all the reporting pieces noted in this article.

Privacy and information security officers will have to evaluate applications and decide if they are going to use a product that can be customized or seek out specific privacy and information security applications already compliant with HIPAA reporting and documentation retention needs. The use of an automated tracking and trending tool can help your organization be successfully compliant with HIPAA documentation and retention requirements. ○

Judi Hofman (judihofman@catholichealth.net) is CHI Regional Privacy Officer – Northwest, Corporate Responsibility, at Catholic Health Initiatives, based in Tacoma, WA.