Compliance
TODAY

Protecting our patients, employees, and communities

an interview with
Lloyd Dean

" Organizations understand that it takes everyone's engagement, at every level, to make a program effective. When you come down to it, compliance is everyone's responsibility. "

See page 18

Compliance
TODAY

by Jay Lechtman, BA, MA

Maintaining HIPAA compliance as OCR modernizes: Two questions to ask

» Privacy breaches — and OCR investigations — continue to rise.

» OCR's modernization efforts for breach reporting provide healthcare organizations an opportunity to think about updating and improving their own HIPAA compliance processes.

» Integrating privacy reporting with other incident reporting activities and systems can improve overall compliance.

» Look at your current privacy reporting, risk assessment, and affected party notification processes to determine where you can automate.

» Don't rely on manual processes to document critical HIPAA compliance activities.

Jay Lechtman (jay.lechtman@riskonnect.com) is Sr. Director, Market Strategy and Development, Healthcare, with Riskonnect in Metro Washington, DC. in */in/jaylechtman*

The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) recently announced updates to its Health Insurance Portability and Accountability Act (HIPAA) Breach Reporting Tool,[1] which gives healthcare providers an opportunity to examine their breach reporting and investigation processes to better meet modern compliance demands.

Lechtman

The HIPAA update comes as the healthcare industry faces a continued increase in the number of breaches, with 329 breaches of 500 records or more reported in 2016 alone. This is an 18% increase from 2015 and the highest total since OCR started publishing major breaches it was actively investigating.[2] Many of these breaches have been triggered in large part by the unprecedented rise in cyberattacks that target provider organizations, placing many on the defensive and prompting them to reexamine both their cybersecurity efforts and privacy compliance processes.

Provider organizations often struggle to meet the 60-day affected party notification requirement because of manual, inefficient processes for initial reporting of events, for risk assessment, and for breach determination as well as the notification process itself.

From my experience with providers across the continuum of care, improving HIPAA compliance efficiency and effectiveness comes down to two questions:

1. Is my breach reporting process integrated with other incident reporting activities?
2. What currently manual steps in the process can be automated?

Is my breach reporting process integrated with other incident reporting activities?

Frontline clinical and other staff in most healthcare organizations are already using automated systems to report incidents

and events related to patient, visitor, and employee safety as well as patient complaints and grievances.

When staff are required to follow a separate process — and use a separate system — to report privacy events and potential breaches, reporting rates can decrease, breaches can go unreported, and critical information can be lost due to reporting delays.

For example, if a medication is given to the wrong patient, particularly in retail clinical settings like pharmacies, two events are occurring simultaneously. The pharmacist or other staff might report the patient identification error, but fail to report the resulting impermissible release of protected health information (PHI). Even if the two errors are identified, having to report them in two different ways into two different systems increases overall reporting time and therefore the risk that busy clinical and support staff will be called away from the reporting process, or wait until the end of a shift and forget time-sensitive information.

Can breach reporting and notification be automated?

Even if integrated with other incident reporting activities and/or systems, when frontline staff are documenting suspected breaches on paper, or completing web-enabled forms that then have to be downloaded and emailed or printed and faxed, it can take days or even weeks for privacy events to get routed to those responsible for HIPAA compliance. These unnecessary delays compress the time allowed for adequate risk assessment, breach determination, and notification of affected parties, if required.

Automation can also improve the efficiency of affected party notification. Even basic mail merge technology allows integration of affected party contact and other data, making it less onerous to generate the required notifications, particularly when hundreds or thousands of affected people can be involved. Automation can also document these activities for you, adding date and time stamps to letter generation and even automatically appending copies of generated letters to patient contact records in your system, making it easy to demonstrate compliance if investigated by the OCR.

Keeping up with the Feds

I'll admit — the recent changes to the OCR HIPAA Breach Reporting Tool are fairly minor organizational and cosmetic improvements. But other federal agencies, such as the Occupational Health and Safety Administration, have made more significant improvements to compliance reporting with the launch of electronic submission portals. I believe it's only a matter of time before HHS OCR follows suit.

Thus, as HHS OCR works to bring HIPAA reporting up to the 21st century, healthcare providers need to ensure that they are following suit. ▣

1. HHS.gov: "HHS Unveils Improved Web Tool to Highlight Recent Breaches of Health Information" July 25, 2017. Available at http://bit.ly/2vcfjxo
2. HIPAA Journal: "Largest Healthcare Data Breaches of 2016" January 4, 2017. Available at http://bit.ly/2CUutHH