WEBINAR Q&A: JUNE 18, 2015

855-733-9888
info@radarfirst.com

Bringing Incident Response and Data Breach Management Out of the Dark Ages

In this webinar, Betsy Madeira, Compliance Administrator for Catamaran took an in-depth look at best practices for managing potential HIPAA privacy and security incidents. Betsy also shared the challenges her organization faces as both a HIPAA business associate and a covered entity, and how her team transformed the organization's intake and assessment capabilities to streamline their incident response process.

Betsy also discussed how her organization utilizes incident response management software to consistently assess incidents, simplify reporting and trending, and increase employee involvement in the process. Here are the questions that were posed by the attendees and answered by presenters Betsy Madeira of Catamaran, and Mahmood Sher-Jan of RADAR®

1 - With the increased value of medical records on the black market what processes have you implemented to make sure your employees don't "steal then sell" patient/member HIPAA?

In support of clear corporate policies prohibiting unauthorized use or disclosure of member/patient PHI, we are seeing organizations implementing products to restrict an employee's ability to download, store, or transmit files containing patient/member data. For example, the use of any plug-in file storage device can be prohibited, and then laptop and desktop computers can be configured to prevent the use of thumb drives, external hard drives, etc. Organizations can also block the transmission of email messages (and attached files) to certain email address types that typically indicate personal use, such as "gmail.com." As an added protection, even legitimate email messages can be scanned for certain key content (e.g., terms such as "date of birth" or "DOB," or drug names) and automatically encrypted prior to transmission.

2 - How do you differentiate roles during an incident? Does someone take the lead? Security or Privacy team?

Any potential HIPAA incident can be reported to either/both the organizational Privacy Officer or the Security Officer. Certain incidents will tend to have a clear bias, and once reported, one team will take the lead, with involvement and support from the other team as needed. If an incident has both Privacy and Security implications, we typically ask that one Privacy and one Security team member be responsible for coordinating their group's investigation, findings, risk assessments, etc. It is not unusual to have both a HIPAA Privacy and a HIPAA Security Risk Assessment documented for one incident. For example, a stolen laptop computer would typically be reported to the IT Help Desk and escalated to the Security Officer and the HIPAA Security Team for immediate action. The HIPAA Privacy Team would also be alerted to the potential HIPAA incident, and would receive all findings in order to determine any incident reporting requirements as either a Business Associate or a Covered Entity.

3 - Does RADAR lend itself to role identification from a workflow perspective?

Yes, RADAR workflow and features are configurable according to the organization's policies and user's role and configured privileges.

4 - Where do you see the Chief Risk Office within the collaboration?

Although this is a very broad question, we believe the equivalent position within some organizations might be Chief Compliance Officer; however, we get the sense that a true "Risk Officer" position would be handling a wider scope (finance, operations, reputation). The Chief Risk Officer would have to rely heavily upon input from both the Privacy and Security Teams. As indicated in the wording of the question, collaboration would be the key.

5 - Do security incidents (e.g. password sharing, unencrypted email, etc.) get reported to the Security Officer or Privacy Officer? Is one or both responsible for investigation and documentation? Whose responsibility is it to address HIPAA incidents?

Both – see #2

6 - Which mitigation response do you find popular and/or most effective?

Mitigation is dependent on the nature of the incident.

7 - Sometimes a treating provider's role may appear to be a business associate and vice versa. Are there any tips for distinguishing "BA" from "not a BA" when the role is not straightforward?

Within certain organizations, the roles are very clear, but we understand that in other environments, such as a physician's office or clinic, the distinction may not be as clear. A Business Associate's obligations are dictated by (1) Federal law, (2) State law, and (3) contractual agreements. If the role is still not clear after legal analysis, and no Business Associate Agreement exists, please seek guidance from counsel. The Covered Entity is ultimately responsible for ensuring its own compliance, and for monitoring compliance by any Business Associates. Any treating providers who are determined to be Business Associates are obligated to safeguard PHI, and to report any potential HIPAA incidents to the Covered Entity provider. The Covered Entity is then obligated by law to assess the incident and, if necessary, to provide notification to both the patient(s) and the Dept. of Health and Human Services (HHS). The role distinction is very important and should be clarified and documented as soon as possible.

8 - How has RADAR impacted your employee discipline process?

RADAR features customizable fields within each incident report. The organization can set up these fields to allow for tracking of employee discipline, and the fields can be included when running a variety of tracking reports. Depending upon the organization's policy, employees may face discipline for involvement in any potential HIPAA incident, regardless of the breach determination. The following is an example:

- Field 1 = Name of Employee(s) involved in the potential HIPAA incident
- Field 2 = Level of Employee Discipline assigned to the employee(s)
- Field 3 = Additional Info – Date Warning Documented or Date Remedial Training Completed, etc.

9 - How do you keep up with laws?

Even with internal resources and awareness, any organization would worry about keeping up with changes and new regulatory requirements. We encourage a team approach including in-house attorneys and paralegals, outside counsel, and the resources built into the RADAR software. State law is a moving target to begin with, and organizations struggle with variations in the definitions of protected information and "breach," staggered incident reporting deadlines, and differences in regulatory involvement (Attorney General, Credit Reporting Agency). An incident may have to be reported as a "breach" under HIPAA, but State law may exempt that same incident if it involves paper, or if it doesn't meet the current definitions. In addition to internal resources, an organization may rely on RADAR and the RADAR team who are constantly monitoring and researching state law and proposed changes, and incorporating them into RADAR's breach guidance engine.

10 - Do you see more incidents? Or patterns of incidents?

It is very important to educate workforce members on the types of incidents that must be reported, and to remind them of their obligation to report potential HIPAA incidents immediately. Employees must understand that the organization is, in turn, obligated to track and report these incidents as a Covered Entity or Business Associate. We find that real-life examples are very helpful.

Workforce members should be reporting potential HIPAA incidents regardless, but simplifying the intake process should make it less painful. RADAR's web-based incident report form makes is easy for anyone to report. Once an incident form is submitted, each incident is personally processed and evaluated, and RADAR supports the risk assessment and breach determination analysis.

Intake = Every employee across the organization has access to RADAR for incident reporting

- Web link opens an online incident report form
- Straightforward and easy to use
- Combination of drop-down fields and text boxes
- Ability to customize many fields (for example, by pharmacy location)
- Allows for upload of relevant documents at intake and after
- Assessment Capabilities (both CE and BA)
- Each incident is assessed in RADAR against established risk factors (already weighted in the system)
- RADAR assists in the performance of incident risk assessment and the determination of whether or not a HIPAA or state Privacy "Breach" has occurred
- Additional input can be added as the investigation progresses, or if there are unusual circumstances or criteria are non-standard