2011 Issue 4

www.ober.com

Why You Need to Worry AGAIN about HIPAA: Seven Practical Tips in the New Electronic Age

By: Sarah E. Swank

In this age of information overload, it is no wonder that privacy incidents are on the minds of regulators, the media and patients. Electronic information in all forms comes at us faster and faster, leaving the recipient without much time to discern among appropriate privacy levels. The increased use of social media and the reality television boom blurred the line between private and public information. People are now posting private information on *Twitter* or *Facebook* without much consideration for their own privacy let alone others.

In the old paper world before HIPAA, people often guarded patient medical records with good old-fashioned common sense. So why, in this new regulated world of laptops, flash drives, mobile devices and electronic medical records, does it appear that patient medical information is less safe? The answer: Our HIPAA policies are stale and our workforce members receive training often created with a focus on paper medical records. In addition, the technology has not caught up with expectations of electronic health record systems to audit access in real time. Electronic health records are a key part of the Accountable Care Act and health care providers and insurers should take note that enforcement will only increase with the pending body of privacy regulations likely to be released by the end of this year.

Below are seven practical tips to prevent your organization from becoming the subject of investigations by the Office of Civil Rights (OCR), Office of the Inspector General (OIG) or State Attorney General, or worse yet, from being required to publicly report under HITECH, draw media attention or lose community and patient trust.

1. Conduct Regular and Routine Audits

Almost gone are the days of walking into the Medical Records Department to conduct an audit of a sampling of medical records. With the increased use of electronic health

records, conducting audits in some ways is simpler than with paper records because of the ability to aggregate data quickly. On the other hand, conducting audits may present problems for covered entities because of the limited reporting ability of certain electronic health record systems. The pure volume and diversity of users in an electronic health record creates additional complexities in audit reviews. Under the proposed accounting rule, covered entities may be required to track access by all persons to all patient records without an exception for TPO (treatment, payment and heath care operations). Below are some considerations when determining an audit plan:

- ***Role-based Access***. Covered entities may want to establish role-based access based on position (e.g., nurse, case manager, and biller) and relationship to the covered entity (e.g., independent medical staff member, IT vendor). A designated department or employee should establish these roles and be responsible for granting access consistent with them. When running an audit, role designation is key in determining the appropriate access and potential for a violation. In certain circumstances, access might be granted in either a view or write capacity with few mechanisms to limit viewing to the minimum necessary amount of information needed for the role.
- ***Scope of Audits***. Covered entities should broaden record audits to include various roles and relationships. The scope of the audit is dependent on whether it is in reference to an incident, a request for an accounting or a routine audit. The scope of audits should be established based on the circumstances and well documented. For example, routine audits should be for a set specific period, while audits triggered by a potential incident may be narrowed to a particular person and/or period.
- ***Frequency of Audits***. Depending on the type of reports run, the appropriate frequency of reporting may vary. For example, access reports may be run in response to an incident or may be monthly reviews of access to family member records. When determining the frequency of running a particular report, a covered entity should take into consideration the ability to timely review the report and act on the results. Covered entities should focus on governmental work plans and recent enforcement activities to determine the scope of annual audits.

- ***Physical Safeguards***. Auditing should extend past audit reports of electronic health medical records and include physical tours of facilities, such as nursing stations, patient rooms and server rooms.
- ***Privilege***. When conducting audits, consult an attorney to determine when certain audits should be done under the privilege of an attorney.

2. Review Incident Reporting Procedures

Incident reporting procedures may seem straightforward, but covered entities may need to take a second look. Most often potential privacy incidents and patient privacy complaints are reported to the privacy officer. The sophistication of privacy officers varies from organization to organization, often due to limited resources of busy clinical settings. In certain instances, the privacy officer may not have the resources to handle large investigations or to distinguish between severities of incidents under the increasingly complex regulatory requirements. Some organizations may be better served by reporting protocols to a compliance office, the legal department or high-level executive that can immediately triage the issue and ensure that the appropriate resources and attention are given to the matter. The sensitivity of privacy incidents and the escalation process became more important under HITECH, which requires covered entities to report certain incidents (i.e., breaches) to the media, regulators and patients.

3. Conduct Timely and Complete Investigations

Privacy investigations are most often triggered by complaints from patients. That being said, investigations may arise as part of routine audits or workforce member reports, and increasingly through government inquiry. In a busy clinical environment with completing priorities, privacy investigations must be complete and timely. Below are some general steps to take when investigating, although each investigation may differ:

- Review related documents (e.g., access reports, medical records, complaint letter)
- Interview witnesses and workforce members
- If appropriate, speak or write to the patient or personal representative for further information
- Revaluate need for additional documents or interviews
- Document investigation scope, method, findings and mitigation plan, including retraining and policy changes

- Consider reporting obligations and respond appropriately
- Respond to government or patient, as appropriate

In addition, covered entities should consider who should conduct the investigation and whether the investigation should be done under the privilege of an attorney.

4. Review and Update Policies and Procedures

The industry is bracing itself for the full impact of HITECH. Currently, HITECH only requires changes to a handful of policies related to the Privacy Rule. HITECH also provided an opportunity to dust off the old policies and evaluate their relevance and effectiveness. In addition, organizations should consider annual reviews and revisions of privacy policies. For example:

- Paper record references, instead of electronic record references
- Patient, media and government reporting requirements under HITECH
- Accounting and auditing
- Role of privacy officer
- Incident reporting
- Social media
- Business associates and business associate agreements
- Use of confidentiality agreements
- Access
- Discipline
- Training requirements
- Updates to departments, titles or phone numbers

Please note that the Notice of Privacy Practice should also be revised consistent to any major policy changes.

5. Revaluate Training

Although we know that training is required under the Privacy Rule, it is not unusual to hear a news story about hospital personal illegally accessing a celebrity's confidential medical information. In 2003, covered entities made a significant push to train their workforce members as required by the then-new HIPAA Privacy Rule. Many

organizations developed standard education with minimum focus on secondary training including job-specific education. Shortly after, covered entities beefed up training related to password sharing and other safeguards required under the HIPAA Security Rule. Education and training should be reviewed to ensure that the unique safeguarding issues around electronic health records, mobile devises, flash drives and access issues are addressed.

In addition, covered entities should update workforce member training for HITECH considerations, including breach reporting obligations. Workforce members themselves do not need to determine if an incident rises to the level of a breach under HITECH. That being said, workforce members, just as in other compliance issues, should be able spot potential issues and be encouraged to come forward with privacy concerns. In addition, workforce members should understand the consequences of breaches, such as reporting requirements and discipline, up to and including termination.

6. Rethink Discipline Determination

Covered entities should review their processes for determining the severity of discipline based on established guidelines. In addition, this process should be based on the relationship with the individual who is found to have violated the covered entity's privacy policies. For example, employee violations may be best handled through the individual's manager and the Human Resources Department. In contrast, independent medical staff member violations may be handled through an already established the Medical Staff process or committee, while business associate violations could be handled through a contracting process or department such as the supply chain. For smaller organizations, the privacy officer may be the one resolving issues for all types of violations regardless of the relationship of the person to the organization. In any event, discipline should be consistent across similar types of incidents and violations, looking at such factors as: (1) harm to the patient or covered entity, (2) intent, (3) lack of training, (4) previous violations or (5) severity of the incident.

7. Mitigation

The mitigation requirements under the HIPAA Privacy Rule are well established. The error some covered entities make is to investigate an incident and never put into place a mitigation plan. Covered entities also may properly identify and document mitigation

steps, but never take the steps to actually correct problems in policies or procedures. Failure to mitigate will expose covered entities to penalties under HIPAA. This is especially true when a covered entity discovers potential remedial measures in the course of an investigation, but fails to take any steps to ensure that a similar privacy incident would not happened again. Mitigation plans should be part of the documentation of a particular investigation, as well as documentation of completion of the mitigation plan.

Act Now

Now is a good time for covered entities to reconsider and reinforce privacy basics with workforce members. More government agencies, such as the OIG, State Attorney Generals and the FBI, are becoming involved in privacy enforcement. New regulations are on the horizon. It is time to dust off the old policies and get ready for this new electronic age.