The Privacy Mindset: Setting Better Boundaries with Third-Party Record Reviewers

By Amy L. Derlink, RHIA, and Elaine Schembari, RN, JD, MBA

Responding to an audit can be hectic and stressful, but HIM professionals must remember to hold external record reviewers accountable to good privacy and security practices.

When you visit the hair salon, take an exercise class, or sit across from a financial planner, you expect them to share your same high level of commitment to reaching your goals. And when you're finally done coifing, sweating, and saving, you expect positive results. But positive results and met expectations aren't just for HIM professionals' personal lives. Similarly, HIM professionals should expect a shared sense of commitment and dedication at the office-even with external third-party auditors and record reviewers.

External reviewers must share your organization's commitment to protecting patient privacy and keeping medical records secure. But as the record of large-scale breaches reported to the Department of Health and Human Services reveals, many external reviewers (especially payers) have experienced massive breaches. Their risks are the same. But what about their safeguards?

As an HIM professional, you must ensure external reviewers maintain good privacy and security practices over the information they are given-whether paper or electronic. But what types of procedures should you have in place? How can you get agreement and compliance with your privacy policies? And what do you do when reviewers try to bully their way past your protocol?

This article explores these issues and provides HIM professionals with practical ways to extend the privacy mindset to their external, third-party reviewers.

Establish Your Policies

The volume of records being requested of providers is on the rise. And the contagion of external auditors and record reviewers has placed increased pressure on HIM staff and the release of information (ROI) process. HIM departments must have policies and procedures that secure these records and ensure a consistent and mutual commitment to patient privacy. As HIM professionals work to hone these policies they should consider three industry drivers:

- Reviewers prefer to review records remotely rather than on site
- Reviewers are trying to avoid reimbursing for records
- HIPAA applies to reviewers, too

Remote versus On-Site Review

The fact that reviewers prefer remote record review is good news for HIM departments struggling to find space for external auditors, but it wreaks havoc on department workloads because of the effort involved in producing the records and ensuring the privacy of the PHI involved.

Remote record review must be addressed in the department's external record review policies and procedures, and it should include such items as:

- Proof of authenticity from the auditing body
- List of requested records
- A copy of the business associate agreement with payer or relevant third party (policies should reflect the provisions of the business associate agreement)
- Proof that the reviewer is an employee or an independent contractor of the auditor
- Proof of the reviewer's identity (e.g., identification badge and valid photo ID such as driver license or passport)
- System access controls and audit logs for any technology utilized to facilitate the remote review
- Internet (IP) address, e-mail address, telephone number, and physical location from which records will be viewed
- Name and contact information of privacy officer at third party

HIM professionals are encouraged to work with IT staff to identify and spell out the technology rules, restrictions, directions, and safeguards for remote access to hospital systems and patient records. In situations where access is being granted to the EHR system, care should be taken with network security and access controls to ensure only the identified and requested patient records and encounters are made available with an electronic "time-out."

By setting automatic time-out features, remote access will shut down and "lock out" the user after a defined period of inactivity. System controls also should ensure the reviewer only has access to the EHR for a specific period of time necessary to conduct the audit (e.g., 15 days). Other levels of controls that should be considered include a restricted connection time (e.g., access is allowed only during normal office hours) as well as a restricted connection location (e.g., restricted to certain IP address ranges).

Alternatively, HIM departments may utilize e-delivery technology within their ROI system or that of third-party ROI providers to give electronic access to only that portion of the patient record requested by the reviewer.

If reviewers are coming on site, the HIM department should have a checklist of items required upon their arrival at the facility, a designated location for record review, and a staff member assigned to assist the reviewers. In addition, if the facility's EHR does not support an appropriate level of system access controls, the HIM department should assign a resource to monitor the reviewer to ensure only the requested patient records are accessed. An audit of records reviewed by the external reviewer should be pulled to ensure only records requested were reviewed.

Finally, whether record access is done via on-site review, remote EHR access, or remote access via e-delivery, only the minimum necessary information should be available to reviewers in accordance with HIPAA regulations. The minimum necessary information represents just those pertinent documents necessary to conduct the review. With remote access and record review requirements shored up, HIM professionals can turn their attention to another area of increasing concern-record reimbursement.

Record Charges

Some reviewers are trying to avoid reimbursing providers and ROI companies for copies of records under the argument that their reviews are covered by the payer-provider reimbursement contract. While certain payer contracts may provide for retrospective record requests, more often they limit the nonreimbursable request language to additional documentation necessary for claims adjudication. It is easy for an HIM professional to confuse a reimbursable, retrospective record request with the nonreimbursable requests for additional documentation at the time of claims submission and payment.

For this reason, HIM professionals should check requests carefully. Any retrospective review, even if being conducted or requested by a legal acting agent, is responsible for reimbursing for reasonable and expected record charges. Bottom line: if the case has been reimbursed and the review is retrospective, a fee should be charged in accordance with state record reproduction rules unless the payer-provider reimbursement contract explicitly states otherwise.

In order to avoid any risk of the reviewer claiming records should be provided at no charge, the HIM department should request the following two items:

- Proof that the requester is a "legal acting agent" of the medical insurer
- A copy of the contract between the provider and the insurer that states medical records are to be released to the insurer at no charge for the purpose of retrospective reviews or audits

If the reviewers are unable to provide this documentation, then records should not be provided until payment is received.

Often the HIM department will find that the contractual language does not provide for release of the records to the payer or a third party but simply states that the records will be made available for review. When this type of language is found in situations where the reviewer would prefer to perform a remote review, the HIM department can negotiate for reimbursement given the operational efficiencies and cost savings the reviewer will realize if they provide access to the records remotely, as was the case for the Mayo Clinic (see below).

Finally, if possible, HIM professionals should take care to include their record rates in the record review policy and managed care contract for each insurer. Customary charges average $10–25 per chart with the maximum set at $50 per record; per page charges with a maximum $50 fee per chart are also commonplace.[1]

Rates should be part of annual negotiations with all insurer and provider contract officers and managed care directors. HIM professionals should work with contracting departments on HIPAA language, policy development, and enforcement. Additionally, HIM staff must be aware of any pre-existing record review terms or contracts related to record review that may supersede any new policies and procedures created.

Extend HIPAA Responsibilities

Like covered entities, insurers and other external reviewers must have policies and procedures in place to prevent PHI breaches under HIPAA. They are business associates under HIPAA and carry the same risks, liabilities, and responsibilities as healthcare providers. (In an early breach, BlueCross BlueShield of Delaware was able to save $150,000 in fines once it demonstrated the existence of a policy and procedure to prevent PHI breach.[2]) It is reasonable and customary for HIM departments to request a copy of the reviewer's HIPAA policies and procedures.

Secondly, before processing a request for records, HIM departments should review the request letter and confirm the requester is a representative of the insurance company or insured. If not an employee of the payer, the reviewer must have a business associate agreement (BAA) in place with the payer and show proof of this agreement.

In addition, the patient consent to treatment form allows records to be shared as part of treatment, payment, and healthcare operations. This consent should be signed by the patient (or patient representative) at the time of treatment, and such authorization documented within the ROI or tracking software at the time of processing third-party audits.

One Hospital's Experience

At the Mayo Clinic in Rochester, MN, an enterprise-wide policy for third-party auditors is in place. This policy is used whenever the reviewer is not already contracted with the organization and the Mayo Clinic is not otherwise obligated to comply with audit requests.

The policy states that all reviewers must be covered under BAAs with the company or payer they have contracted with to review records, and these agreements require complete compliance with HIPAA requirements. Furthermore, as a business associate with Mayo, a direct BAA with Mayo is in place for the respective payer. If both of these criteria are not met, Mayo holds the reviewer liable for any breach based on contractual arrangements and BAAs.

One interesting stipulation in the Mayo policy is that on-site reviews or audits are no longer allowed. This is certainly a sign of the times and a trend in managing external reviewers.

Strength through Policy

Mayo reports great success in keeping reviews under control since enacting the enterprise-wide policy. The categories within the policy include:

- Scheduling the audit
- Authorization for disclosure of medical record information
- Documentation

- Standards of care
- Fee information
- Audit fee
- Release of final audit report
- Mayo response to final audit report
- Audit procedures
- Related documents and references

While every HIM department's policy will vary, these general topics will cover the three focus areas (remote review, record charges, and HIPAA responsibilities) and set the stage for better management and collaboration with external, third-party reviewers.

Notes

1. IOD Incorporated. Internal research.
2. "Insurer Must Show Policy to Prevent PHI Breach." *HIPAA Weekly Advisor*, January 26, 2009. www.hcpro.com/HIM-227000-866/Insurer-must-show-policy-to-prevent-PHI-breach.html.

Amy L. Derlink (aderlink@iodincorporated.com) is privacy and compliance officer at IOD Incorporated in Green Bay, WI. Elaine Schembari (schembari.elaine@mayo.edu) is section head, quality and compliance, at Mayo Clinic Rochester in Minnesota.

Article citation:
Derlink, Amy L; Schembari, Elaine. "The Privacy Mindset: Setting Better Boundaries with Third-Party Record Reviewers" *Journal of AHIMA* 83, no.3 (March 2012): 26-29.