Medical Records: Signed, Sealed and Secure

By Kay Hardgrave

As patients are diagnosed and treated in University hospitals and clinics, the Health Information Management (HIM) department collects and stores information about each patient through use of medical records. The HIM is responsible for coding, transcribing, maintaining and protecting the medical records of all patients. Accuracy, completion and timeliness of medical records directly impacts medical decision making and accuracy of billing. Access to the records 24 hours/7 days a week adds to the complexity. Unauthorized access to records with Protected Health Information (PHI) increases privacy and security risks and potential non-compliance with the Federal Health Insurance Portability and Accountability Act (HIPAA). The above may result in penalties and negative publicity. Additionally, medical identity theft is on the increase. For all these reasons, the safeguarding of medical records is critical.

The process of developing the medical records audit program should be risk driven – ideally, the result of a brainstorming session. See Table 1 for an example. Identify the applicable risks based on the background and scope. Consider the following:

- Are the medical records for patients in a hospital and/or clinics? Are the records housed in one department?
- Are the medical records primarily physical patient files, electronic medical records (EMR), or a hybrid? Many organizations will be in a hybrid state as they expand the use of EMRs. For example, radiology and lab reports, pharmacy and medical administration records may convert to EMRs, while the physician order entry system may still be physical.

This article focuses on an audit for a hybrid state of records, primarily physical charts. However, as hospitals and clinics convert to EMRs, the shift in audit risks will require you to go back and audit with different steps and related testing. Audit objectives include the following:

- Assess the overall general controls over the environment; and
- Evaluate the controls over physical security, procedures for release of records, third party contracts, timeliness of physician chart completion, and training.

Although transcription and coding accuracy and efficiency are important areas, this article does not address these except for a limited step for coding. The emphasis of the program below is compliance with HIPAA, contracts, policies and laws.

Overall Controls and Physical Security

In order to assess the controls over the environment, especially security and privacy, it is important to conduct a walk-through and observe! Request a guided tour of every HIM location. In a hospital, an emergency room may have a satellite HIM location. Do not forget older records stored in the basement. During the tour, complete the developed checklist along with follow-up questions. If there are multiple locations, use a separate checklist for each one. Comparing the

environment in various locations assists in identifying inconsistencies procedures and conditions. See Checklist.

Tests of Controls over Security and Privacy

1. *Data regarding Physical Access – Badge System*

How is management monitoring for suspicious activity regarding access? How do you know who has access, when, or the length of time spent in area after business hours? How do you verify the effective date access was terminated? Can a transferred or terminated employee use their badge to access the department, especially after-hours? Verify with the administrator of the University badge system how quickly an employee's badge is deactivated and whether the employee has to turn in the badge for deactivation to occur. If the badge system is a stand-alone system and not integrated with the University badge system, how does deactivation occur? Obtain and review a report of access data. Compare data with the list provided by management of approved users and their access hours. Review list of users and dates of access; compare to terminated/transferred employees and effective date of termination/transfer, especially from the HIM department.

2. *Follow the Records - Test how patient privacy is maintained during transport of medical records.*

Identify the general routes and procedures for physical records that are in transit – either collected for HIM or sent from HIM to another location; e.g. delivered to a clinic. Are records transported within HIM because a functional area is physically in another area; e.g., coding or transcription? Accompany staff members on routes and observe practices to protect patients' privacy from prying eyes. Do they consistently cover the records? Are loose records carried in their hands, or in an uncovered cart or bin? If they are being carried through a facility, can someone read patient information such as social security numbers, medical procedures, and even patient names if he is standing close in an elevator? If a vehicle is used, are windows tinted or passengers prohibited?

3. *Software – Information Security Assessment*

Identify any subsystems that feed into and are integrated for the creation and tracking of the patient's medical record. Ask your IT department to assist with an information security assessment on software that is used by HIM and/or other departments for medical records. Some of the questions may include:

- Are inactive user IDs deactivated?
- Are the audit software controls turned on? Are audit logs reviewed?

4. *Tests of Filing Accuracy*

Select a sample of patient files; test for misfiled protected health information – the inclusion of another patient's medical record.

Select a sample of medical record numbers from populations of patients discharged and patients recently admitted, to determine the recorded location of the record. Test if the record can be located quickly on the first attempt. If it is a physical file, observe the pulling of the chart. If it is in HIM, could the staff locate the file on the first attempt? If it is out on a hospital floor, could it be located quickly at the nursing unit? If an electronic medical record, observe the staff utilizing the software to retrieve the record.

Select a group of files. Determine if they are filed per department standards; e.g. physical files filed by last four terminal digits.

Procedures for Release of Information (ROI) – Copies of medical records are requested from external groups - patients and attorneys - as well as internal requests from the denial of claims (appeals) staff and patient billing services needing records to seek reimbursement. Determine whether the procedures are compliant with HIPAA and any state laws that govern the rates charged for the copies. Determine if the Release of Information (ROI) function is handled in-house or it has been outsourced. If outsourced, see section on Third Party Contracts.

Tour the ROI area and observe the following for HIPAA compliance:

1. Is there adequate privacy for patients?
2. Are required notices posted regarding HIPAA and complaints? Even if outsourced, the complaint notice should provide the name and phone number of the HIM director.

Inquire as to the performance of the area or current contractor. Have there been complaints from patients as to a delay in receipt of records that may result in patient dissatisfaction? Since the primary source of the contractor's revenues is external customers, there may be delays in processing internal requests. Check with internal customers - denials and patient billing services - regarding the timeliness of responses. The delay in processing denials results in slower or potentially reduced reimbursement for services. Ask them for a report indicating the number of days outstanding for their requests and required follow up.

Observe how the ROI staff handles the security and privacy of records in transit.

Cash Handling/Credit Cards - If payment is not the responsibility of third party contractor, then evaluate the controls. Also determine compliance with credit card policies to protect the personal information; i.e. the credit card number.

Review all third-party contracts with companies that access, review or perform functions with medical records for the following:

1. HIPAA training responsibility
2. Financial arrangement – Do the terms reflect the intent of HIM management with the third party as described to you? Is the University providing space? Are there revenue sharing or payment terms? Compare terms to invoices for appropriate approvals and accuracy. For example, a company providing ROI services may charge for internal requests, usually for the number of copies that exceed a threshold per month at a per page rate. Review invoices per

page rate to contractual rate. If the company has overcharged a few cents more per page, the recovery amount can add up to thousands of dollars!

3. Does the contract require a quality assurance program to be in place? If so, review their procedures. For example, if a company is assisting with a backlog of filing loose paper, what is done to verify filing accuracy?
4. Standard audit clause
5. If there is a contractor that is not in a direct contractual relationship with the University, but is reviewing patient charts as part of their duties, verify there is a Business Associate Agreement to cover their chart review for HIPAA purposes.

Timeliness/Delinquencies of Physicians completing charts

To be in compliance, physicians must complete charts before patients' bills are dropped; i.e., claims are filed for payment. What is the policy on deadlines? How is the timeliness or delinquencies of chart completion monitored by HIM? Is the staff proactive by sending physicians reminders that charts are incomplete? If so, review the number of days that lapse after the discharge date before reminders. How often do medical delinquencies occur? What are the enforcement practices for delinquencies?

Training - Are new employees HIPAA trained before they begin? Check training logs. Ask for documented desktop procedures and if additional training is offered.

Coding - Two quick steps regarding coding accuracy include:

1. *Emergency Room* - Does the HIM coder perform an independent reconciliation of the ER medical records against the ER daily patient log to ensure that the hospital has captured the charges to reimburse the hospital for its services?
2. *External Audit Reports* - If external audit reports are performed on the coding accuracy, review for the most current report's results and recommendations. How does HIM follow up with the recommendations or if a coder has less than satisfactory performance? Has HIM presented the report to senior management and/or a compliance committee?

Conclusion

Internal Audit's added value of an audit focused on compliance is to help ensure that medical records are signed, sealed and secure from inappropriate access. This will mitigate the risk of the University's exposure to potential penalties and negative publicity.