Case Reveals How Easily Patient Confidentiality Can Be Breached

Jenna Peterson, a 20-year-old college student, made an appointment to be seen by Susan Grant, M.D., one of the partners at Mountainside Family Medicine Associates. Jenna had been seeing Dr. Grant for a few years. Dr. Grant was also the long-time family practitioner for Jenna's mom and older sister.

On this visit, Jenna said she would like to get a prescription for birth control pills. They discussed other contraception options, as well as the risk and benefits of each and decided that "the pill" would be Jenna's best option. After reviewing Jenna's medical history and performing a brief physical examination, Dr. Grant gave Jenna a six-month prescription for Ortho-Novum 10/11, along with educational materials on oral contraceptives. She told her to schedule a six-month follow-up appointment over summer break.

When Jenna checked out with the front office, she told the billing office that she did NOT want this visit submitted to her mother's insurance. Instead, she would pay for the visit herself because she didn't want her mother to know the reason for the visit. The billing clerk said that she would send Jenna a bill because the practice's billing system was undergoing a software upgrade. Jenna asked that the bill be sent to her college address.

About two weeks later, Mrs. Peterson had a routine appointment with Dr. Grant. When she checked in, she stopped by the billing office and asked the insurance clerk to check a notice of claim statement she recently received from her insurance carrier about a visit by Jenna. Mrs. Peterson said, "I know Jenna hasn't been here because she's away at school." The clerk said she'd check on the claim and should have information for Mrs. Peterson by the time she was done seeing Dr. Grant. Mrs. Peterson was then taken back to an exam room for her appointment.

While seeing Mrs. Peterson, Dr. Grant inquired about the Peterson family and mentioned that "Jenna has really blossomed into a beautiful, intelligent young woman." Mrs. Peterson thanked Dr. Grant and asked, "When did you see Jenna?" Dr. Grant unthinkingly said, "Oh, a couple weeks ago when she was in for her appointment." When Mrs. Peterson questioned why Jenna had been seen, Dr. Grant realized she had said too much. She hemmed and hawed a bit, and finally suggested that Mrs. Peterson talk to Jenna.

Despite Mrs. Peterson's insistence that she had a right to know why Jenna was seen, Dr. Grant refused to provide additional details. Mrs. Peterson was clearly angry with that response and stormed out of the exam room. On her way out, she stopped at the billing office, and the insurance clerk confirmed that Jenna was in for an appointment on the day in question and that the claim was correct.

Allegations and Claims Investigation

Jenna Peterson's right to privacy was obviously compromised by both Dr. Grant and her billing office. Both Jenna and Mrs. Peterson terminated their relationship with Dr. Grant and Mountainside Family Medicine Associates as a result of the incident.

Jenna initially threatened to sue the practice for a breach in patient confidentiality, HIPAA non-compliance and emotional distress. Though she never followed through on the suit, she filed a formal HIPAA Privacy Violation Complaint against both the physician and the practice with the Office of Civil Rights (OCR).

The investigation into the case found Dr. Grant at fault for revealing that Jenna had been seen as a patient. Her disclosure was not malicious—just not well-thought out. However, even if Dr. Grant had not mentioned Jenna's visit, her privacy would have been breached when the practice filed the claim with Mrs. Peterson's insurance, in spite of Jenna's arrangement to the contrary. Dr. Grant admitted she should not have mentioned Jenna to Mrs. Peterson, particularly after the physician had reassured Jenna that her request for "the pill" would go no further.

The breakdown in the billing office was blamed on the fact that the system was "offline" the day of Jenna's visit. The clerk's note concerning Jenna's instructions about her bill never made it into the system, and the claim was automatically submitted to Mrs. Peterson's insurance company. However, Jenna received a bill from the office several weeks later, and she submitted her payment. This created other problems for the practice because Mrs. Peterson's insurance had also paid on the claim.

The OCR's investigation into this complaint found several areas where the practice, as a covered entity, was not in compliance with HIPAA Privacy regulations. The practice had no specific policies and procedures in place

for protecting patient confidentiality, other than a record release policy.

Although the practice had a named privacy officer, the worker had never performed or been assigned any duties in that regard. Neither had the practice performed a risk assessment to determine where patient privacy safeguards were lacking or could be improved.

The practice's new staff orientation program did not cover the issue of patient confidentiality in any detail, nor was there any specific staff training program in place with regard to HIPAA and patient privacy. The OCR mandated HIPAA training of the entire practice staff—professional and ancillary. This was required to take place immediately and with ongoing, regularly scheduled refresher training sessions held.

The OCR also suggested the practice perform a root-cause analysis to determine what steps the practice and Dr. Grant should have been taking to prevent the unauthorized disclosure of information. Based on the results of the risk assessment, the practice developed and implemented appropriate corrective and preventive measures.

What Can We Learn?

A physician's duty to protect confidential patient information long predates laws and regulations like HIPAA or HITECH that mandate the protection of patient health information (PHI). In fact, it is addressed in the Hippocratic Oath:

> *Whatsoever things I see or hear concerning the life of men, in my attendance of the sick or even apart therefrom, which ought not be noised abroad, I will keep silence thereon, counting such things to be as sacred secrets.*
>
> Oath of Hippocrates, 4th Century, B.C.E.

Protecting patient confidentiality has long been recognized as inherently important to the practice of Medicine. It is necessary to foster the free exchange of information that guides the physician in the diagnosis and treatment of a patient. It also is critical to establishing trust and rapport, which are essential to a strong physician/patient relationship, patient satisfaction and good clinical outcomes. And once that duty is breached, it can be next to impossible to rebuild the physician/patient relationship or regain the patient's trust.

Patients must feel confident that personal information they share with physicians or staff will not become public knowledge or be released to third parties without their authorization and/or consent. Without that assurance, a patient may be reluctant or unwilling to provide personal or sensitive information that could be critical to his or her care. The diagnostic process can be difficult enough when a physician has access to all available information. If pieces of information are missing, the patient's health and treatment outcome may be jeopardized.

The physician's duty of confidentiality extends to each staff member, and every employee has an inherent duty to protect patient information. No patient information may be released without the patient's express permission (with the exception of emergencies). Unauthorized disclosure can result in malpractice allegations, along with HIPAA violations.

Unfortunately, this case demonstrates how easily patient confidentiality can be violated. The disclosures of Jenna's care had not been done maliciously, criminally or even consciously. There was no sophisticated technology involved. The root cause was simply a lack of understanding about the physician and staff's role in protecting patient confidentiality and a failure to have policies and procedures in place to prevent a breach.

The issue of protecting patient confidentiality and PHI has renewed importance with the long-awaited publication of the final privacy rules on January 17, 2013. The HIPAA Final Omnibus Rule[1] clarifies and defines changes to the original HIPAA of 1996 regulations necessitated by the Patient Safety and Quality Improvement Act of 2005 and the Health Information Technology for Economic and Clinical Health Act (HITECH) Act of 2009.

According to HHS, the final rule greatly enhances a patient's privacy protections, provides individuals new rights to their health information, and strengthens the government's ability to enforce the law. The HIPAA Omnibus Rules actually encompass four final rules:

1. Modifications to the HIPAA Privacy, Security and Enforcement Rules.
2. HIPAA Enforcement Rule changes.
3. Breach Notification for Unsecured Protected Health Information under HITECH.
4. Modification of the HIPAA Privacy Rule as necessitated by the Genetic Information Nondiscrimination Act or "GINA."

Among other things, the Final Omnibus Rule:

- Expands the liability of a covered entity for HIPAA non-compliance of its business associates and now hold business associates

[1] Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule, Fed Reg. 78(17): 5566- 5702, January 25, 2013.

liable for the non-compliance of their subcontractors.
- Expands individuals' rights to electronic copies of their PHI.
- Gives individuals the right to restrict disclosure of PHI for treatment they paid out of pocket.
- Incorporates the increased and tiered HITECH civil money penalty structure.
- Strengthens limitations of disclosure of PHI for marketing and fund-raising purposes.
- Modifies the privacy notice requirements for statements on PHI uses and disclosures that require authorization.

The HIPAA Omnibus Final Rule is effective March 23, 2013. Covered entities and businesses must comply with the applicable requirements by September 23, 2013. Covered entities and business associates will have up to one year following the compliance date to modify their business associate agreements in accordance with the requirements of the final rule.

Risk Management Recommendations

- **Give patient confidentiality high priority** among all professional, support, janitorial, security, IT and ancillary staff. The duty of confidentiality extends to all—no exceptions.
- **Have a dedicated privacy officer, as mandated by HIPAA**. This privacy officer will bear responsibility for:
    - Being the "go to" person for questions about what information may be released and to whom.
    - Developing, implementing and disseminating practice policies and procedures.
    - Educating staff on privacy issues.
    - Investigating and reporting privacy breaches or patient complaints.
    - Overseeing the practice compliance with the HIPAA Privacy Act.
- **Require staff to sign a confidentiality agreement when first employed.**
- **Include the topic of patient confidentiality in staff orientation** and in ongoing HIPAA training programs for all employees. The goal is to increase staff awareness of the need to protect PHI and how easily patient confidentiality can be breached (e.g., an overheard conversation, an open patient chart, a message left on a patient's answering machine, or an appointment list posted in patient areas).
- **Implement policies and procedures that address all aspects of patient information.** This includes its collection, storage, release, archive and destruction—in both hard-copy and electronic formats.
- **Put in place mechanisms to flag protected PHI or information a patient has requested not be shared.** This can be more difficult with electronic medical records and automated billing systems. One provision in the HIPAA Final Rule allows patients who have paid "out of pocket" to request that their information **NOT** be disclosed to insurance companies or others.
- **Implement a practice policy for the storage of e-PHI on mobile devices** and their physical removal from the practice. Lost or stolen electronic devices containing e-PHI continue to result in serious breaches of patient information.
- **Develop consequences for employees who breach patient confidentiality** (from written warnings for minor offenses up to termination of employment for repeated and/or serious offenses). Ensure consistent enforcement for all employees. The OCR can also assess monetary fines against individual employees for PHI breaches found to be malicious and for personal gain.
- **Review the expanded requirements of the HIPAA Final Omnibus Rule immediately** and address what modifications will be needed to comply by September 23, 2013. Specifically, physicians, privacy officers and the practice legal counsel should address the impact of the Current Notice of Privacy Practice and Business Associates Agreements on the practice.