Should Employees Be Allowed to Access to Their Own Information?

There are Multiple Aspects to Consider Before Making This Decision

The Health Insurance Portability and Accountability Act (HIPAA) privacy rule grants individuals the right to access their information that is created, collected, and/or maintained by the health care providers and health plans that provide services to the individual. The regulation further stipulates that access must be provided in the form or format requested by the individual, if it is readily producible in such form or format. [45 C.F.R. 164.524.]

One might argue, then, that individuals who are employed by a covered entity should be allowed to directly access their own information via the covered entity's computer systems. There are multiple aspects to consider, however, before making the decision to allow or prohibit employees from accessing their own information.

HIPAA Rules of Use

Unlike many predecessor state privacy laws that mainly dealt with disclosure, the HIPAA privacy rule added a new dimension by governing use of protected health information (PHI). A covered entity may use PHI for its own treatment, payment, and health care operations. In addition, there are limited allowances for fundraising and research.

There is no allowance, however, to use PHI for “personal reasons.” There's no argument that a health care provider's employees may not use the PHI of family members and friends for personal reasons. One could argue, however, that HIPAA does not grant an allowance for anyone acting in the role of a covered entity's workforce to use any PHI for personal reasons — even one's own information.
ACHIEVING COMPLIANCE

Adequate training is critical to a health care organization’s success in complying with HIPAA and other privacy regulations. Employees must fully understand the limits to their use and disclosure of PHI. Patients depend on this and will not trust an organization with their information if the organization fails to maintain a high level of compliance.

In terms of accessing information in an electronic health record (EHR) system, the optimal approach to promote compliance is one simple rule: Only use protected health information to perform your job. Period. No exceptions. Granting employees access to their own information for their own personal purposes would create an exception to this simple rule. One might suggest that exceptions increase complexity, and complexity makes compliance more challenging.

PATTERNS OF MISBEHAVIOR

Assuming active auditing is in place to ensure appropriate use of the EHR system, a covered entity may detect patterns of use (and misuse). If your organization permits access to one’s own record, an audit of user activity for those who have done so would be wise. It may reveal a pattern where the employee first accesses his or her own record, and then goes on to access family members, coworkers and other acquaintances. Even “good” employees might be tempted to take a mile when given an inch.

SYSTEM PRIVILEGES

The electronic health record (EHR) may be one component of a larger, integrated clinical information system. For example, the integrated clinical information system in the physician practice setting may include medication and other orders, charges, billing, registration, and scheduling in addition to visit notes, test results, and other clinical information. A nurse’s job duties may include updating a medication profile or entering prescription renewals on behalf of a physician. If an organization allows employees to access their own records in such a system, there is an opportunity for the user with the necessary system privileges to modify his or her own medication profile, add refills or renewals, etcetera.

This would be similar to a bank allowing employees to access their own accounts, with the possibility that several zeroes might be added to enhance the worth of a savings account. If a system has the capability to prevent such activity or to alert the security team, this likely is not a concern. If that is not true, however, the most prudent approach may be to employ the administrative safeguard of a policy that prohibits employees from accessing their own record. Access should then be monitored, to ensure compliance with the policy.

MINORS’ RECORDS

Depending upon a given state’s laws regarding access to minors’ records, there may be certain information or encounters that require the minor’s authorization before access can be provided to a parent. Access requires a gatekeeper, then, who can review the information available and determine if any information exists that requires the minor’s consent before access is provided.

Some employees may not understand the complexities of these laws and may expect the law grants them the right of access. Even if such access is prohibited by a policy, employees may be confused because the covered entity has already allowed access to their own records as a patient right under HIPAA. Why wouldn’t the same hold true for their minor children’s records?

SINGLE STANDARD OF CARE

The most common reason employees desire access to their own electronic record is because they want faster access to test results. If this is necessary to promote high-quality health care, shouldn’t this type of access be made available for all patients rather than just patients who are employed by the health care organization? Web-based patient portals provide an excellent solution, whereby all

CONTINUED ON PAGE 80
ners interested in creating and obtaining approval from the government for new types of gainsharing arrangements. After years of restricting decisions, these OIG opinions appear to put substance ahead of form and may be a harbinger that hospitals will be allowed to begin operating like other businesses.

Endnotes
* Poul Anderson (1926-2001), writer
1. Any proposed gainsharing arrangement also should be evaluated in light of the federal and state anti-kickback statutes, the physician self-referral prohibitions, and potential private incurrence by tax-exempt organizations.
2. See OIG Advisory Opinion No. 05-01 issued January 28, 2005; OIG Advisory Opinion Nos. 05-02, 05-03, and 05-04 issued February 10, 2005; and OIG Advisory Opinion Nos. 05-05 and 05-06 issued February 18, 2005.
3. Notably, the OIG stated that its decision not to impose sanctions in connection with these proposed gainsharing arrangements is consistent with its July 1999 Special Advisory Bulletin, where it found similar arrangements to be inappropriate.
4. The federal anti-kickback statute prohibits offering, paying, soliciting, or receiving remuneration to induce or reward referrals reimbursable by a federal health care program.

Protected Health Information
Continued from 66

patients have equal rights and access to the information that has been identified as beneficial for delivery directly to the patient.

Patient Versus Employee Role
Employees who are treated at their own workplace expect their employer to maintain strict delineation between the roles of employer versus health care provider. HIPAA requires the same so that supervisors do not cross the line by helping themselves to their employees’ protected health information as part of the employment relationship.

This sounds simple but can be challenging. Consider the employee who becomes sick at work and is taken into an exam room and is seen by a clinic physician. Does the supervisor know the employee is sick because she is the supervisor or because she is the health care provider? This is hard enough, without further muddying the waters by allowing employees to mix their roles of employee versus patient.

Again, a simple rule makes this far less challenging. When you are an employee, act like an employee. When you are a patient, act like a patient. Patients do not have direct access to the health care organization’s internal clinical information systems.

Conclusion
HIPAA does not clearly prohibit allowing employees to directly access their own electronic health record. There are several arguments, however, that prohibiting this activity may lead to overall better compliance with privacy policies and laws.