Identity Proofing: Just a Fancy Name for Verification?

Save to myBoK

by Barry S. Herrin, FACHE, Esq.

Among the issues being brought to the fore in the movement to electronic health records (EHRs) is identity proofing. However, this is the same issue healthcare providers have faced for as long as patients have been contacting providers in ways other than face-to-face communications. This article explores the legal foundation for identity proofing, discusses some of its thornier issues, and identifies some of the tried and true solutions for verifying identities in both the paper and EHR environments.

The Legal Framework

The HIPAA privacy rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.[1] The privacy rule calls this information "protected health information" (PHI).[2]

Every healthcare provider, regardless of size, that electronically transmits PHI in connection with certain transactions is a "covered entity" and is required to comply with the privacy rule, whether it electronically transmits these transactions directly or uses a third party (like a billing service) to do so on its behalf.[3]

Among the protections afforded by the privacy rule, a covered entity may not use or disclose PHI, except either as the privacy rule permits or requires or as the individual who is the subject of the information (or the individual's personal representative) authorizes in writing.[4] A covered entity must obtain the individual's written authorization for any use or disclosure of PHI that is not for treatment, payment, or healthcare operations or otherwise permitted or required by the privacy rule.[5]

A covered entity may not condition treatment, payment, enrollment, or benefits eligibility on an individual granting an authorization, except in limited circumstances.[6] An authorization must be written in specific terms. It may allow use and disclosure of PHI by the covered entity seeking the authorization or by a third party.

All authorizations must be in plain language and must contain specific information regarding the information to be disclosed or used, the person(s) disclosing and receiving the information, the expiration of the authorization, the right to revoke the authorization in writing, and other data.[7]

Finally, in addition to reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of PHI in violation of the rule (including the obligation to limit incidental use and disclosures), the privacy rule requires a covered entity to "verify the identity of a person requesting [PHI] and the authority of any such person to have access to the [PHI]… if the identity or any such authority of such person is not known to the covered entity."[8,9]

For electronic PHI, the security rule requires covered entities to protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required by the privacy rule.[10] For our purposes, we will focus only on the technical safeguard provisions of the security rule. This requires covered entities to adopt and implement policies and procedures for controlling access to electronic PHI through their IT functions, including unique user identification, and suggesting the need for automatic log-off functions and the encryption and decryption of PHI.

Covered entities are also required to provide audit controls, adopt policies and procedures to ensure data integrity, and implement policies and procedures to verify the identity of any person requesting access to electronic PHI.[11]

Technology Adds Complexity

When initial encounters with a patient or other authorized representative are conducted in person, providers can gather traditional proofs of identity and can at that point introduce the patient or representative into the facility's electronic system by assigning a password or other method enabling remote access, information requests, and similar functions.

However, when a party first requests access to or disclosures of PHI through technology, complexities occur. This is nothing new. Providers have long agonized over whether to release information over the telephone to persons representing themselves as patients or "responsible parties" (a term that has no real legal meaning in the HIM context).

HIPAA complicates this routine scenario in several ways. First, the privacy rule requires that covered entities account for certain PHI disclosures.[12] However, this accounting does not have to include disclosures to the patient or to persons pursuant to a written patient authorization. Even with the electronic records acts passed by state and federal governments, it is far from certain whether any computer security protocol and password assignment routine (however robust) will be viewed as the equivalent of written authorization.

Second, the data points required in a valid authorization may also cause significant problems for the record keeper. For example, in order to accommodate the expiration date of the authorization, a process must be developed to disable passwords or record copies upon expiration.

Finally, there is the problem of verification. The HIPAA privacy rule also requires that covered entities verify the identity of persons wishing to access their own PHI or authorizing the release of PHI outside the provider's control.[13] In addition, the security rule requires that covered entities adopt procedures to verify and authenticate the identity of a person seeking to obtain access to electronic PHI.[14]

Some Modest Proposals

In the rush to embrace EHR systems, we should not lose the institutional knowledge we have gained in implementing access to paper records, both face-to-face and remotely. First, when we interact with patients in person, we should continue to obtain copies of government-issued identification that bear a patient signature. This will permit lay comparison of signature on written requests to release information.

In this process, we should also gather some other piece of identifying information that only the patient will know, such as mother's maiden name, elementary school attended, or a password. Doing so can eliminate the difficulties of interacting over the telephone with unknown persons, creating a way of verifying patient identification in a low-tech environment.

Second, information requests from third parties purporting to act for the patient are especially challenging when prior proof of identify has not been received in writing (e.g., requests received via the Internet, telephone, or fax). It is difficult, if not impossible, to identify a satisfactory compliance solution.

If we adopt a patient identifier process as described above, and the patient gives a third party this information, we now have to impute authorization without a satisfactory writing, and the provider's privacy rule burden technically is not met. In addition, the HIPAA security rule requires an audit control capability, as well as access validation procedures for all access attempts.[15,16]

Requiring a unique identifier for each person requesting remote access (including physicians and family members) could be too cumbersome and is likely to limit a patient's desire to disclose information, even if it would facilitate continuity of care. However, such a system is the only way to satisfy the current security rule requirements, and it is a recommendation presented to the confidentiality, privacy, and security work group of the American Health Information Community (AHIC).[17]

Third, both paper and electronic systems must identify and segregate episodes of care to which certain patient representatives are not permitted access. Records of self-referring minors, minors who have gained the age of majority, and patients who have objected to certain persons having access all must have electronic "flags" as counterparts to existing paper systems.

Fourth, proving the identity of the requesting party is not enough. Providers must still obtain satisfactory evidence that the patient representative has the authority to gain access to the information sought, and strictly speaking the only way to do this is to obtain official documentation of the representative's status prior to any remote interaction with such person. AHIC has not addressed this problem in its recommendations.

Regardless of the recent buzz over identity proofing, the burden on healthcare providers remains the same. Providers must still engage in basic information gathering, preferably in person and in writing, to prove that the person authorizing or requesting the release of records is who he or she purports to be.

In addition, providers must continue to insist on proof that persons requesting access to records on behalf of patients truly have the authority to do so. Adopting an electronic process without attending to these “old-fashioned” details will only permit inappropriate release to occur faster and more frequently.

Common Problems in Identity Verification

Two common challenges in identity verification involve minor children and deceased patients. Electronic record systems add to the complexity.

Minor Children

Parents presenting their minor children for treatment in person will have many documents indicating their parental status, such as a healthcare benefit card showing the minor as a dependent. Collecting a copy of the parent's picture identification and pegging it to the minor's chart might assist the provider, as these identification cards also contain a facsimile signature against which the provider can compare the signature on a request for records.

In situations involving divorce or custodial disputes, often the parent with the decision-making authority (or the court order) will share this authority (and the noncustodial parent's limitations) with providers. In some cases, providers have a copy of the minor's birth certificate to assist in identifying the parents. Foster and child custody arrangements have their own formal legal documentation. These fairly routine procedures have been in place with most providers for years, and there is no reason to re-engineer the process of parent identification.

The real problems with minor patients arise in two contexts. First, there are circumstances under which minors can legally self-refer for care without parental permission. In most states, these include outpatient voluntary mental health treatment, alcohol and drug testing and treatment, treatment for sexually transmitted diseases, and pregnancy and childbirth counseling and treatment. Records of such treatment should not (absent the consent of the minor patient) be made available to the patient's parent, regardless of how well the provider may know the parent. Consequently, protocols must treat these records differently when access is requested.

Second, when minor patients reach the age of majority, they are ordinarily entitled access to the medical records created when they were minors. Rarely do providers have any information establishing the identity of minor patients, as their focus prior to that time has been on establishing the identity of the parents.

Deceased Patients

The HIPAA privacy rule requires covered entities to verify a personal representative's authority to act on behalf of a patient, but the privacy rule defers to state law to establish who is a "personal representative" (subject to some restrictions involving patient safety).[1] The Centers for Medicare and Medicaid Services state that "covered entities should continue to identify personal representatives as they have done in the past," according to a FAQ on the subject posted on the HIPAA section of its Web site.

In the case of deceased patients, every state has a formal process by which the executor or administrator of the estate can be identified. Providers should insist on official documentation from the court evidencing this status. The same rationale holds true for durable powers of attorney for healthcare-the provider should insist on having a copy of this document in the patient's chart before interacting with this person as the patient's authorized representative.

However, in many states, the surviving spouse or other descendants have access to the records of deceased patients, without regard to their status as the personal representative of the patient's estate. Such status does not usually have any accompanying official documentation, and providers do not routinely request copies of birth or marriage certificates to prove that a person is the surviving spouse or child. In skilled nursing facilities, there may be a person with whom the facility must communicate regarding resident care and treatment, but this person often has no official authority or status to act on behalf of the resident under state law.

Note

1. Health Insurance Portability and Accountability Act of 1996. Public Law 104-191. 45 CFR § 164.514(h).

Notes

1. Health Insurance Portability and Accountability Act of 1996 (HIPAA). Public Law 104-191. 45 CFR § 160.103.
2. Ibid.
3. Ibid.
4. HIPAA 45 CFR § 164.502(a).
5. HIPAA 45 CFR § 164.508.
6. For example, a covered-entity physician may condition the provision of a physical examination to be paid for by a life insurance issuer on an individual's authorization to disclose the results of that examination to the life insurance issuer, or a covered healthcare provider may condition treatment related to research (e.g., clinical trials) on the individual giving authorization to use or disclose the individual's PHI for the research. HIPAA 45 CFR § 164.508(b)(4).
7. HIPAA 45 CFR § 164.508(b).
8. The Office for Civil Rights privacy rule guidance suggests, among other things, "securing medical records with lock and key or pass code, and limiting access to keys or pass codes." HIPAA 45 CFR § 164.502(a).
9. HIPAA 45 CFR § 164.514(h)(1)(i).
10. Recall that the privacy rule contains the majority of physical security requirements for all PHI. 45 CFR § 164.530(c).
11. HIPAA 45 CFR § 164.312.
12. HIPAA 45 CFR §§ 160 and 164.
13. HIPAA 45 CFR § 164.514(h)(1).
14. HIPAA 45 CFR § 164.312(d).
15. HIPAA 45 CFR § 164.312(b).
16. HIPAA 45 CFR § 164.310(a)(2)(iii).
17. These recommendations were presented in a working draft dated January 23, 2007, and can be found on AHIC's Web page at www.hhs.gov/healthit/ahic/materials/01_07/cps/draft_recs.doc.

Barry S. Herrin *(barry.herrin@smithmoorelaw.com) is an attorney with Smith Moore LLP, based in Atlanta, GA.*

Article citation:
Herrin, Barry S.. "Identity Proofing: Just a Fancy Name for Verification?" *Journal of AHIMA* 78, no.5 (May 2007): 54-55;60.