# Providing Nonemployees with Access to an Electronic Health Record

Save to myBoK

*By Thomas A. Lucas, MA, and April M. Carlson, MBA, HCISPP, CFE*

Healthcare organizations often must provide nonemployees with access to their electronic health records (EHRs) for treatment, payment, and healthcare operations. A wide range of nonemployees may need this access.

Some may work under the organization's direct control, such as visiting physicians, unpaid interns, volunteers, contractors, and temporary agency staff. Others may work at the direction of outside organizations. Physicians who work for other employers but who see patients at the organization may need access, as may the nurses and surgical technicians who assist them. Some nonemployees may need access for purposes other than treatment, such as coding professionals, scribes, transcriptionists, and the employees of organ procurement organizations. External auditors from the Department of Health and Human Services (HHS), the Centers for Medicare and Medicaid Services (CMS), and insurance companies may also need to see the EHR. Referring providers are another important group of external users of the EHR.

While giving EHR access to these nonemployees is essential to treating patients and conducting business, it poses a risk to the privacy of protected health information (PHI). A survey conducted in 2016 by Soha Systems found that 63 percent of data breaches resulted directly or indirectly from third party access.[1] To safeguard the privacy of their patients' health information, healthcare organizations must put in place procedures to minimize the risk of improper access to PHI by nonemployees who have EHR access.

## Strengthening Internal Policies

The implementation of a new EHR gave Mayo Clinic (Mayo)—a multispecialty group practice with major campuses in Rochester, MN; Scottsdale, AZ; Phoenix, AZ; and Jacksonville, FL—an opportunity to strengthen its policy and procedure governing nonemployee access. Mayo began replacing its multiple EHRs with a single integrated EHR in 2017. Mayo formed a task force to address the issue of nonemployee access to the new EHR. The task force included representatives from the Center for Connected Care, Health Information Management Services (HIMS), Information Technology, Management Engineering & Internal Consulting, the Office of Information Security, the Privacy Office, and Provider Relations. The charge of the task force was to develop and implement a policy and procedure for provisioning, monitoring, and terminating nonemployee access to the EHR.

The HIPAA Privacy Rule requires healthcare organizations to identify "those persons or classes of persons, as appropriate, in its workforce who need access to protected health information to carry out their duties; and for each person or class of persons, the category or categories of protected health information to which access is needed and any conditions appropriate to such access" (45 CFR § 164.514(d)(2)(i)).

Workforce is defined as "employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate" (45 CFR § 160.103).

The Privacy Office went beyond this minimum requirement by classifying not only the members of its workforce but also those outside its workforce who needed access to PHI. Persons needing access to PHI were divided into seven user groups. The first group is made up of Mayo employees and students in Mayo schools, such as staff consultants, residents, scientists, medical students, and allied health staff.

The second group includes Mayo workforce members who are not Mayo employees, such as visiting physicians, visiting scientists, visiting students, unpaid interns, volunteers, contractors, and temporary agency staff.

The third group is composed of healthcare providers who are not part of the Mayo workforce but whose credentials have been confirmed by Mayo. This group includes providers employed by other organizations who see patients at Mayo clinics or hospitals or via telemedicine.

The fourth group includes the support staff of these providers, such as nurses and surgical technicians.

The fifth group includes nonemployees who need access for purposes other than treatment, such as coding professionals, scribes, transcriptionists, and employees of organ procurement organizations.

The sixth group is made up of external auditors from insurers and government agencies such as HHS and CMS. Group seven includes nonemployees who need read-only access to the EHR for treatment purposes, such as referring physicians.

Once the nonemployees had been classified, the task force developed a procedure for gathering information about prospective nonemployee users, deciding whether to give them access, providing approved users with access to the appropriate categories of PHI, training them in the EHR and privacy regulations, obtaining their signatures on a user agreement, monitoring their access, and terminating their access when it is no longer needed.

All nonemployees who work at Mayo have a Mayo-employed supervisor. The supervisor is responsible for confirming the identity of the nonemployee, deciding whether access to the EHR is needed, and applying for access. The supervisor begins the application process by logging in to the Mayo network and submitting a Nonemployee Account Request Form to HIMS. The form requests information that identifies the proposed user and his or her job responsibilities. It also asks whether EHR access is needed, and if so, whether read-only or read-and-write access is necessary.

When HIMS receives the completed form, it decides—with the assistance of the Privacy Office—whether to approve access. If the nonemployee works for a business associate, as defined by the HIPAA Privacy Rule, HIMS checks to see if Mayo has a current business associate contract that meets the requirements of the Privacy Rule (45 CFR §§ 160.103, 164.502(e), 164.504(e)). HIMS then assigns each approved user to one of the seven user groups and sends the form and the user group number to Enterprise Account Management (EAM), which maintains the Person Database, a repository of information about all persons who have access to Mayo's electronic systems. Using the information on the form, EAM creates a record in the Person Database for the nonemployee. EAM then gives the nonemployee a user ID and password permitting access to the Mayo network.

Once the information about the nonemployee is in the Person Database and access to the Mayo network has been granted, the supervisor can apply for access to the EHR. This is done in an access management system. This system requires the supervisor to select a role for the proposed user. The role determines the categories of PHI to which the nonemployee will have access. In accordance with the HIPAA Privacy Rule, access is limited to the "minimum necessary to accomplish the intended purpose" (45 CFR § 164.502(b)). The access management system then creates an EHR user record and assigns the EHR security templates for the role. The nonemployee is then trained to use the EHR and follow the HIPAA Privacy Rule. Finally, the nonemployee signs an agreement stating that he or she will use the EHR for business purposes only.

The final step is to monitor the nonemployee's use of the EHR and terminate it when it is no longer appropriate. This is done in four ways. First, the EHR automatically terminates the access of external auditors after a limited period of time, which is set by HIMS. Second, EAM sends the supervisor an email every 90 days asking if the nonemployee still has a relationship with Mayo. If the supervisor responds that the relationship no longer exists, EAM terminates access to the EHR and the Mayo network. Third, the access management system sends an email to the supervisor annually asking if the nonemployee still needs access to the EHR. If the supervisor responds that the nonemployee no longer needs access, the access management system terminates it. Thus, the EAM team confirms that the nonemployee's relationship with Mayo still exists, while the access management system confirms that the relationship requires EHR access.

Fourth and finally, the Privacy Office monitors the nonemployee's access to ensure that it is appropriate. A nonemployee may be treating Mayo patients and have a legitimate need to see patients' medical records. If the nonemployee is also looking at a neighbor's records for personal reasons, however, the Privacy Office will terminate the nonemployee's access, take appropriate corrective action, and conduct a breach risk assessment.

Mayo now has a process in place that allows nonemployees to access its EHR when necessary for treatment, payment, and healthcare operations, but minimizes the risk of an improper disclosure of PHI.

# Note

[1] Soha Systems. “Third Party Access is a Major Source ofData Breaches, Yet Not an IT Priority.”

*Thomas A. Lucas (lucas.thomas@mayo.edu) is a principal health systems engineer, and April M. Carlson (carlson.april@mayo.edu) is the privacy officer at Mayo Clinic.*

**Article citation**:
Lucas, Thomas A; Carlson, April M. "Providing Nonemployees with Access to an Electronic Health Record" *Journal of AHIMA* 88, no.11 (November 2017): 46-47.