AMA
AMERICAN MEDICAL ASSOCIATION

"Break-the-Glass" EHR Functionality

Are restrictions requiring "break-the-glass" EHR functionality to access employees' patient records necessary for all employees of a health system?

DEBUNKING THE MYTH

The HIPAA privacy rule does not specifically require that health care organizations universally apply extra restrictions on access to patient records of employees or their immediate family members with "break-the-glass" EHR functionality.

Additional information

Break-the-glass, or break-glass functions require an EHR user to enter additional authentication information and documentation of a specific business reason for accessing a patient record before they can enter a patient's chart that is subject to heightened restrictions. Each access is tracked and monitored by designated security or compliance staff. The feature, which is enabled if an organization requests it from their EHR vendor, is intended to further ensure protected health information (PHI) privacy for certain types of patients by restricting access to only those individuals involved in the patient's care.

Many health care employees (and their immediate family members) are patients at the health systems in which they work, receiving health care services from physicians and other clinicians they may work with. Some organizations, in an effort to protect those patient records from unnecessary access by other employees, may institute heightened restrictions on all employee health records, as well as patient records for the employees' immediate family members, requiring the additional step of using the "break-the-glass" function to access the record. When applied universally, such restrictions can create unnecessary onerous steps and inefficiencies for the clinicians treating patients who work in the health system. Over the course of a patient's time with a health system, this extra effort of validation can take clinicians' time away from other important patient-facing tasks. Employees of a health system are able to request such restrictions on access to their own medical records.[1]

Security of patient data is paramount and should be a top concern for all health systems. Protecting sensitive patient information must also be balanced with workflow efficiency. The HIPAA privacy rule does not require specific restrictions on accessing patient records, but it does require health care organizations take reasonable steps to ensure patient information is only accessed when, and by whom, it is necessary to provide care or services. There may be other ways to provide these safeguards that do not create unnecessary administrative burden. Health care organizations should consider state-specific restrictions when determining how to implement additional protections on certain types of health records. Some federal restrictions, such as those regarding substance use disorder records, should also be considered.

Break-the-glass protocols can also be effective for ensuring security when sensitive patient information is shared outside the health system and accessed in certain environments (e.g., external emergency departments). These protocols require external users—those not affiliated with your health system—to document a clinical reason before accessing restricted records.

Key takeaway

By de-implementing universal heightened restrictions for health system employee patient records that require the use of a "break-the-glass" function to access those records—and only enabling this feature for those who have requested such restrictions—health care organizations can increase efficiency for physicians and other clinicians treating those patients.

References

1. U.S. Department of Health and Human Services (HHS). HIPAA FAQ 3026: Under HIPAA, may an individual request that a covered entity restrict how it uses or discloses that individual's protected health information (PHI)? HHS. December 28, 2022. Accessed January 13, 2025. https://www.hhs.gov/hipaa/for-professionals/faq/3026/under-hipaa-may-an-individual-request-that-a-covered-entity-restrict-how-it-uses-or-discloses-that-individuals-protect-health-information/index