U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

21st Century Cures Act Guidance: Remote Access to PHI for Activities Preparatory to Research

May a researcher access PHI through a remote access connection as a review preparatory to research?

Yes, under certain, specified conditions, and provided reasonable and appropriate security safeguards are in place, a researcher may access protected health information (PHI) through a remote access connection as a review preparatory to research. However, covered entities must comply with the relevant standards in both the Privacy Rule and Security Rule before providing access to PHI through a remote access connection for preparatory research purposes.

Under the Privacy Rule, covered entities are permitted to use or disclose PHI for reviews preparatory to research, if the researcher provides representations that satisfy section 164.512(i)(1)(ii). The required representations must, among other things, provide that no PHI will be removed from the covered entity by the researcher (e.g., physically taken out of a facility, or downloaded and retained on the researcher's device) in the course of the review. Remote access connectivity (i.e., out-of-office computer access achieved through secure connections with access controls and authentication) involves a transmission of electronic PHI, which is not necessarily a removal of PHI under the Privacy Rule, even though the covered entity is providing access to the PHI, and the PHI is being accessed and/or used by the researcher. However, although the access to PHI through a remote access connection is not itself a removal of PHI, the printing, downloading (with a limited exception), copying, saving, data scraping, or faxing of such PHI, or any other means by which a researcher outside the covered entity might control or retain the PHI, would be considered to be a removal of PHI from a covered entity.

Covered entities that permit their workforce or other researchers to access PHI via a remote access connection must also comply with the Security Rule's requirements for appropriate safeguards to protect the organization's electronic PHI. For example, the standards for access control (45 CFR § 164.312(a)), integrity (45 CFR § 164.312(c)(1)), person or entity authentication (45 CFR § 164.312(d)), and transmission security (45 CFR § 164.312(e)(1)) require covered entities to implement policies and procedures to protect the integrity of, and guard against the unauthorized access to, electronic PHI. The standard for transmission security (45 CFR § 164.312(e)) also includes addressable specifications for integrity controls and encryption. With respect to encryption, this means that the covered entity generally must implement encryption to protect electronic transmissions of PHI as well as protecting PHI at rest, if reasonable and appropriate. In the event that the covered entity determines that the use of encryption is not reasonable and appropriate in a particular circumstance, it must document its specific rationale for not encrypting despite technological advances and growing cybersecurity concerns, identify the available and appropriate equivalent alternative means to protect electronic PHI as it is transmitted, and implement a reasonable and appropriate solution.

When can a covered entity rely on the representations of a researcher that the researcher will not remove PHI from the covered entity when the researcher requests to access PHI through a remote connection for activities preparatory to research?

The Privacy Rule permits a covered entity to rely on representations from certain persons requesting PHI, if such reliance is reasonable under the circumstances. 45 CFR § 164.514(h)(2)(i). In the case of a request by a researcher to access PHI remotely for activities preparatory to research, this means that, among other things, the risk that the researcher will remove PHI from the covered entity without authorization should be assessed in order to determine whether it is reasonable to rely on the researcher's representation that the PHI will not be removed. The covered entity should determine whether its reliance is reasonable based on the circumstances of the particular case.

For example, a covered entity may conclude that it can reasonably rely on representations from researchers who are its employees or contractors that they will not remove PHI from the covered entity because their activity is manageable through the covered entity's employment or contractual relationship and related policies establishing, for example, sanctions for the misuse of PHI and privacy- and security-related requirements for its use. On the other hand, where the researcher has no relationship with the covered entity, the covered entity may conclude that it cannot reasonably rely on the researcher's representations that PHI will not be removed from the covered entity, unless the researcher's ability to remove PHI is managed in some other way, for example, with guarantees that technical safeguards are in place that provide view-only access to ePHI and prevent copying, printing, saving, data scraping, faxing, downloading, or any other means by which a researcher outside the covered entity might control or retain the PHI.

Does the automatic downloading and/or temporary storage of PHI to a researcher's computer constitute removal of PHI from the covered entity?

Yes, unless safeguards are in place to prevent any individual, outside of the covered entity, from retaining the downloaded PHI. A covered entity must conduct a risk analysis when selecting an appropriate remote access solution to permit access to its PHI. If the covered entity deploys a solution that automatically downloads files containing PHI to an outside researcher's computer system or device for temporary storage, the covered entity must implement safeguards to mitigate the associated risk and ensure that the PHI downloaded to the third party device is not retained. For example, the entity may conclude that it is reasonable to rely on representations from researchers who are its employees or contractors that downloaded PHI is securely encrypted and that they will securely purge (i.e., immediately and permanently delete) any temporary PHI files from their devices as soon as the PHI is no longer needed for the review preparatory to research. However, if the covered entity concludes that it cannot reasonably rely on a researcher's representations (e.g., where the researcher has no connection to the covered entity), the covered entity should implement a different, more secure remote access solution, such as one that prevents copying, printing, downloading, saving, faxing, or data scraping, and automatically encrypts or securely purges temporarily stored data when the remote access connection is terminated. Examples of more secure remote access solutions include a presentation engine or

virtualization (such as a Virtualized Desktop Infrastructure or VDI) to provide access to data from remote sources without downloading data locally.

Is a covered entity liable for a HIPAA violation if a researcher who gains access to PHI for reviews preparatory to research then removes PHI from the covered entity (e.g., by retaining data accessed remotely)?

A covered entity's liability in such circumstances depends on the facts and circumstances of a particular case. Factors to consider in determining whether the entity failed to comply with one or more provisions of the HIPAA Rules would include, but are not limited to, for example: whether the entity obtained the required representations from the researcher that PHI would not be removed in the course of the review; whether reliance on the researcher's representations was reasonable under the circumstances; the extent to which the entity implemented reasonable and appropriate administrative, physical, and technical safeguards to prevent the researcher from impermissibly retaining PHI; and (if the researcher was a workforce member) whether the entity imposed sanctions for any impermissible use of PHI. In addition, if an impermissible use or disclosure of PHI occurred, the covered entity may be subject to the requirements of the HIPAA Breach Notification Rule.