Changes to Privacy Protections in the Face of COVID-19

Although the country is beginning to reopen, the COVID-19 virus remains a very real threat, and it continues to have a significant impact on all aspects of the healthcare system. In the wake of the coronavirus outbreak, the Department of Health and Human Services acted swiftly to make a number of changes to federal privacy protections, as well as issuing updates and guidance, in order to improve the nation's ability to share information to provide safe and effective care.

Although most of the changes are specific to the crisis and thus not intended to be permanent, there are no explicit expiration dates, and many have argued that some of the adjustments – particularly that related to telehealth – should remain in place even after the virus has been contained.

Below we summarize these changes to the privacy protections for health data and provide links to additional resources.

Temporary Changes to HIPAA

HIPAA, the federal law governing the use and disclosure of patient health information, is recognized as the foundation of consumer privacy protections. At the start of the pandemic, HHS issued three HIPAA-related waivers to provide flexibility to providers on the front lines of treating COVID-19 cases and ease fears regarding potential liability for HIPAA violations. To date, it is unclear how long these waivers will remain in place. These include:

1. Sanctions and penalties waived against covered hospitals
    - Section 1135 of the Social Security Act allows HHS to waive the provisions of a variety of healthcare laws and regulations – such as sections of the Emergency Medical Treatment and Labor Act (EMTALA), Medicare telehealth requirements, and requirements related to the disclosure of patient health information – during certain public health emergencies.
    - HHS implemented this waiver in March, and guidance has been updated as recently as June 15.

2. Relaxed enforcement of telehealth services
    - The HHS Office of Civil Rights (OCR) announced in March that it would exercise its enforcement discretion to not impose penalties for provider noncompliance with the HIPAA Privacy and Security Rules in connection with the good faith provision of telehealth during the COVID-19 public health emergency.
    - Under this waiver, providers can use non-HIPAA covered technologies such as Zoom, FaceTime, or Skype to provide care.

3. Allowances for new types of testing sites
    - Community-based testing sites (CBTs) are semipublic testing sites that are set up in places such drive-through sites or those set up in parking lots. The notification of

enforcement relaxes some of the HIPAA regulations regarding PHI that is typically handled in a private setting. However, providers still must implement the minimum necessary rule when handling PHI.

Permanent Changes to Privacy Protections for Substance Abuse Data

The CARES Act made permanent changes to the so-called "Part II Regulations" governing the confidentiality of patient records related to treatment of substance abuse disorders, more closely aligning them with HIPAA and adding important new protections. Notably, the changes provide that once information has been disclosed pursuant to patient consent, that information can be re-disclosed by a covered entity without additional consent for purposes of treatment, payment or health care operations, as permitted by HIPAA. The CARES Act also adds new antidiscrimination protections for information obtained from Part II records.

Guidance to First Responders Using Personal Health Information

OCR issued guidance intended to help clarify how law enforcement, paramedics, and other first responders can use and disclose PHI in responding to COVID-19. Notably, this guidance does not constitute an actual change to HIPAA rules, but provides helpful additional direction.

For more information on privacy policy and related updates, visit the Privacy page in the ehealth resource center. https://www.ehidc.org/resources/privacy-cybersecurity?tid=155