COVID-19 raises HIPAA privacy, security issues

By Mercer's Katharine Marshall, Cheryl Hughes and Kaye Pestaina
April 6, 2020

In this article

Employers sponsoring group health plans still need to heed federal privacy and security obligations under the Health Insurance Portability and Accountability Act (HIPAA) during the COVID-19 pandemic While the HIPAA rules and other federal laws allow sharing protected health information (PHI) in limited circumstances during nationwide public health emergencies, plan sponsors should review HIPAA's limits on PHI use and disclosure, as well the plan's related policies and procedures. Plan sponsors should also review recent COVID-19 guidance from the Department of Health and Human Services (HHS) relaxing some HIPAA rules. In addition, updated guidelines from the Equal Employment Opportunity Commission (EEOC) address employers' COVID-19 concerns and relevant standards on medical inquiries and confidentiality under the Americans with Disabilities Act (ADA) and state privacy laws. This GRIST reviews basic HIPAA rules and related COVID-19 agency guidance, which is likely to evolve as the pandemic continues.

HIPAA baseline

Title II of HIPAA sets privacy, security and standardization requirements for health data maintained or transmitted by health plans (including employer group health plans) and other covered entities:

- Privacy rules. HIPAA's privacy rules require covered entities to limit the use and disclosure of PHI. Covered entities must apply appropriate safeguards but can use PHI (limited to the minimum amount necessary) without an individual's authorization for certain activities, including treatment, payment and healthcare operations. The privacy rules also establish numerous basic rights for individuals with respect to their PHI.

- Security rules. HIPAA's security rules set out steps that covered entities must follow to secure electronic PHI (e-PHI). Covered entities must establish a security infrastructure, protect any IT systems that store or transmit e-PHI, and ensure business associates safeguard e-PHI.

Privacy reminders

Because HIPAA applies only to covered entities and their business associates, any information about an employee's health that an employer might obtain is subject to HIPAA only if received in the context of a group health plan. Information about an employee's exposure to or contraction of the virus that an employer receives from the group health plan is subject to HIPAA. In contrast, information about COVID-19 symptoms, exposure or diagnosis that an employee shares with a coworker or supervisor (who is not part of the health plan's workforce) is not subject to HIPAA.

The HHS Office for Civil Rights (OCR) has issued a bulletin reminding covered entities about their HIPAA obligations in light of the coronavirus outbreak. Disclosing PHI necessary for treatment, including care management and coordination, does not require obtaining the patient's authorization. Covered entities also can disclose PHI without the patient's authorization to:

- A public health authority, such as the Centers for Disease Control (CDC) or a local health department
- A foreign government agency at the direction of a public health authority
- Persons at risk of contracting or spreading a disease or condition, if authorized by law when necessary for public health intervention
- A patient's family members, relatives, friends or others involved in patient's care, but only if one of these conditions applies:
  - The patient has given verbal permission or is reasonably presumed not to object.
  - The patient is unconscious or incapacitated, and professional judgment concludes that the disclosure is in the patient's best interest.
- Anyone as necessary to prevent or lessen a serious and imminent threat to the health and safety of a person or the public

A few of these permitted PHI disclosures without individual authorization merit a closer review in light of the present pandemic.

Disclosure to public health authorities. PHI may be disclosed without individual authorization to the CDC and to state and local health authorities that are collecting information about the spread of COVID-19.

This means a covered entity can disclose PHI to those authorities on an ongoing basis, as needed to report cases of COVID-19 exposure and suspected or confirmed cases of COVID-19. If authorized by the business associate agreement (BAA), a business associate can also make these disclosures to public health authorities on behalf of a covered entity.

Disclosure to persons at risk. Covered entities can disclose PHI without individual authorization to persons at risk of contracting or spreading the virus, but only if a state law (such as a duty-to-notify law) authorizes such disclosures to prevent or control the spread of disease. Before making this type of disclosure, covered entities should carefully consider applicable state laws and regulations.

Disclosure to prevent or lessen a serious threat. The HIPAA privacy rule permits disclosing PHI without individual authorization to others in a position to lessen or prevent a serious imminent threat, if the disclosure is consistent with applicable state laws and regulations. Health professionals typically make this type of disclosure relying on professional judgment about the nature and severity of the public threat.

Minimum necessary limit always applies. Even when PHI disclosure without individual authorization is permissible, covered entities can disclose only the minimum necessary information. Relying on the CDC's or another public health authority's statement that the requested information is the minimum necessary is likely reasonable under the circumstances.

Disclosures to the media. HIPAA does not permit disclosing PHI to the media without first obtaining written authorization from the individual or an authorized representative.

Other laws restricting disclosure of medical information

Besides HIPAA, other laws — like the ADA and state privacy laws — may restrict the disclosure of medical information. Updated EEOC guidance on pandemic preparedness in the workplace and the ADA discusses a variety of situations in which an ADA-covered employer can inquire about employees' COVID-19 symptoms. The guidance states that any information from those inquiries that an employer receives and maintains is subject to the ADA's confidentiality rules.

Because public health authorities have acknowledged community spread of COVID-19, examples of reasons why an employer might inquire about COVID-19 during the pandemic emergency — while abiding by ADA confidentiality rules — include:

- To send home an employee with COVID-19 or symptoms associated with it
- To determine if employees who report feeling ill at work or call in sick have COVID-19 symptoms, such as fever, chills, cough, shortness of breath or sore throat

- To measure employees' body temperature
- To obtain information considered necessary by the CDC and state/local public health authorities before permitting an employee's return to the workplace after travel to certain locations, whether for business or personal reasons

Employers should note that these special EEOC rules on medical inquiries apply only during the pandemic emergency.

Considerations for working remotely

Many employees are working remotely in response to government stay-at-home orders or employers' voluntarily closing workspaces to reduce spread of the virus. Remote work can create some privacy and security challenges. The HIPAA rules apply to PHI, regardless of where covered entities' employees and business associates are located. A covered entity's HIPAA policies and procedures likewise apply equally to employees working in the office and from home.

Coordination with a multidisciplinary team of information technology, legal, operational and other professionals may be necessary to mitigate risk associated with working from home unexpectedly. A few key points to keep in mind include:

- Employees accessing PHI should have private workspaces.
- PHI should not be accessed on shared devices, including printers.
- Hard copies of PHI should be stored securely or shredded.
- Computers or other access to PHI should be physically secured and not left unsecured or unattended.
- Access to PHI should still be safeguarded with features like unique user IDs, passwords, automatic logoff or screen lock, and encryption tools.

Covered entities may want to conduct new HIPAA training, focusing on how privacy and security policies and procedures apply in the remote environment. Covered entities should also consider whether any new service providers facilitating remote work require business associate contracts. Keep in mind that breach notification rules continue to apply, and inadequate or untimely breach notifications can trigger penalties.

HIPAA and COVID-19

Given the ongoing and evolving nature of the COVID-19 pandemic, HHS continues to issue guidance easing certain HIPAA rules or explaining how those rules apply during the pandemic. In addition, the

Coronavirus Aid, Relief and Economic Security (CARES) Act (Pub. L. No. 116-136) directs HHS to issue guidance on PHI disclosures that addresses compliance with existing HIPAA regulations and any new policies taking effect due to the national emergency. This guidance will likely reflect HHS's broader ability to waive HIPAA rules due to the public health emergency.

Limited waivers for hospitals

The secretary of HHS has announced limited waivers of certain HIPAA privacy sanctions and penalties in response to the declaration of a nationwide COVID-19 public health emergency. Existing law (Pub. L. No. 108-276 and 42 USC § 1320b-5) gives the federal government authority to waive certain HHS requirements during a national emergency. The HIPAA waivers for hospitals apply only for 72 hours from the time a hospital implements its existing disaster protocol.

Under the waivers, HHS will not impose sanctions and penalties on covered hospitals that do not comply with the HIPAA privacy requirements to:

- Obtain a patient's consent before consulting with family or friends involved in patient's care
- Honor a patient's request to opt out of the facility directory
- Distribute the notice of privacy practices
- Honor a patient's request for privacy restrictions
- Honor a patient's request for confidential communications

When the public health emergency ends or the 72-hour waiver period expires, whichever occurs first, the hospital must again comply with all HIPAA privacy requirements.

Waivers may extend to group health plans. The broader HHS authority granted in the CARES Act could allow the agency to issue waivers that apply to group health plans — in addition to healthcare providers — during a national emergency.

Disclosure for public health oversight

HHS has announced it will not impose HIPAA penalties on healthcare providers or business associates engaging in good-faith PHI uses and disclosures for public health and health oversight activities during the nationwide COVID-19 public health emergency. Current regulations allow a HIPAA business associate to use and disclose PHI for public health and health oversight purposes only if expressly permitted by the BAA or required by law. Under the new nonenforcement policy, the OCR will not penalize business associates that provide requested PHI or related data analytics to federal and state public health

authorities, state and local health departments, and state emergency operations centers during the COVID-19 national emergency, even if the BAA does not expressly authorize this activity.

This penalty relief applies only if the business associate notifies the covered entity about the PHI disclosure within 10 days. The nonenforcement policy will remain in effect until the HHS secretary declares the public health emergency no longer exists or the declared public health emergency expires, whichever occurs first.

Disclosure to first responders

The OCR has issued guidance providing examples of when covered entities — including group health plans — may disclose the PHI of an individual who has been infected with or exposed to COVID-19 to law enforcement, paramedics, other first responders and public health authorities. Plans sponsors should review the guidance to refresh their knowledge of these standards.

Relief for telehealth

Under March 17 guidance, the OCR will not impose penalties during the public health emergency on providers using certain telehealth remote communications that do not meet HIPAA's privacy, security and breach notification requirements. Examples of these communication technologies include popular video chat applications like Apple's FaceTime, Facebook Messenger, Google Hangouts, Zoom and Skype.

This enforcement discretion presumably applies to all HIPAA covered providers delivering care to any patient, including those covered by private commercial plans and employer-sponsored plans. More information is available through a set of OCR FAQs. The office will issue a public notice when this enforcement discretion related to telehealth ends.

Civil rights, HIPAA and COVID-19

A recent OCR bulletin reminds entities subject to Section 1557 of the ACA — generally those receiving HHS funding for health programs — and Section 504 of the Rehabilitation Act about those laws' anti-bias protections. Both laws prohibit discrimination on the basis of race, color, national origin, disability, age, sex, exercise of conscience or religion.

The OCR is particularly concerned that people who have disabilities or limited English skills or need religious accommodations might get put at the end of the line for health services during the pandemic. To avoid that outcome, entities covered by Section 1557 should generally ensure — if resources allow — that they:

- Provide effective communication with individuals who are hearing or visually impaired

- Provide meaningful access to programs and information for individuals with limited English proficiency
- Deliver emergency messages in plain language — and in the languages prevalent in the affected area — and in multiple formats
- Address the needs of individuals with disabilities
- Respect requests for religious accommodations in treatment and access to clergy or faith practices

Some actions or accommodations may not be required if they fundamentally alter the nature of a program, impose an undue financial and administrative burden, or pose a direct threat.

Next steps for employers

Stay tuned for future guidance. As the COVID-19 pandemic continues to unfold, employers should stay tuned for rapidly evolving guidance from HHS and other agencies regarding the HIPAA privacy and security rules and related group health plan obligations.

Stay the course on HIPAA privacy and security compliance. Group health plans have not received any general relief from HIPAA's privacy and security rules. Employers with health plan employees working remotely or with limited operations must continue to focus on HIPAA privacy and security compliance and report any security breaches if necessary. State privacy laws also continue to apply.

Any medical testing requires careful review of ADA rules. Before establishing any type of medical test for employees, including taking body temperatures, employers should review with employment counsel the EEOC's related ADA rules and guidance.

Avoid discrimination. Any entities that receive HHS funding and are subject to the ACA's Section 1557 rules should carefully review the new guidance on avoiding prohibited discrimination under the federal civil rights laws.

Review substance use disorder (SUD) disclosure reforms. Unrelated to the current public health crisis, the CARES Act has significantly changed the Public Health Service Act's confidentiality requirements governing the use and disclosure of certain SUD information (42 US § 290dd-2). These requirements are often referred to as "Part 2," which is where related regulations appear in Title 42 in the Code of Federal Regulations. The law generally doesn't apply to group health plans, unless they have obtained Part 2 information from covered providers and want to redisclose it. Employers adopting innovative value-based purchasing arrangements have had concerns about Part 2's more restrictive consent requirements. The CARES Act addresses these concerns, revising the statute to align many of its requirements with

HIPAA and directing HHS to update existing Part 2 regulations accordingly. The revised rules will apply to SUD information uses and disclosures starting 12 months after the legislation's March 27 enactment.

Related resources

Non-Mercer resources

- HHS webpage on HIPAA, civil rights and COVID-19 (HHS)
- Notice of enforcement discretion under HIPAA: Use and disclosure of PHI by business associates for public health oversight (HHS, April 2, 2020)
- Civil rights, HIPPA and the coronavirus disease 2019 (COVID-19) bulletin (HHS, March 28, 2020)
- Pub. L. No. 116-136, the CARES Act (Congress, March 27, 2020)
- HIPAA and emergency preparedness, planning and response (HHS, March 27, 2020)
- COVID-19 and HIPAA: Disclosures to law enforcement, paramedics, other first responders and public health authorities (HHS, March 24, 2020)
- Pandemic preparedness in the workplace and the Americans with Disabilities Act (EEOC, March 21, 2020)
- FAQs on telehealth and HIPAA during the COVID-19 nationwide public health emergency (HHS, March 20, 2020)
- Notification of enforcement discretion for telehealth remote communications during the COVID-19 nationwide public health emergency (HHS, March 17, 2020)
- COVID-19 and HIPAA bulletin: Limited waiver of HIPAA sanctions and penalties (HHS, March 2020)
- HIPAA administrative simplification (CMS, Feb. 12, 2020)
- Bulletin: HIPAA privacy and novel coronavirus (HHS, Feb. 3, 2020)
- COVID-19 public health emergency declaration (HHS secretary, Jan. 31, 2020)
- HIPAA and public health (HHS, June 16, 2017)
- HIPAA FAQs for professionals (HHS)

Mercer Law & Policy resources

- Roundup: COVID-19 resources for employers (March 31, 2020)
- CARES Act boosts telehealth, makes other health, paid leave changes (March 27, 2020)
- Healthcare law and policy outlook for 2020 (Feb. 18, 2020)
- Top 10 compliance issues for 2020 health and fringe benefit planning (June 25, 2019)

Other Mercer resources

- Stay informed on coronavirus (updated regularly)

Note: Mercer is not engaged in the practice of law, accounting or medicine. Any commentary in this article does not constitute and is not a substitute for legal, tax or medical advice. Readers of this article should consult a legal, tax or medical expert for advice on those matters.