HIPAA COMPLIANCE DURING THE COVID-19 PANDEMIC

Last Updated: April 13, 2020

TABLE OF CONTENTS

Hall Render privacy attorneys are monitoring the federal government's response to the COVID-19 pandemic and the impact on HIPAA compliance. Health care providers must stay up to date on HIPAA obligations during public health emergencies as well as opportunities to postpone or waive certain requirements during the COVID-19 pandemic. **Although these federal changes may offer some relief, covered entities should consider applicable state law as well. For example, state law encryption requirements. For further information or assistance, contact your Hall Render attorney.**

BE AWARE: Bad actors are taking advantage of the COVID-19 pandemic. In one instance, OCR warns of a bad actor calling covered entities and posing as an OCR investigator attempting to access PHI. To verify that an individual is legitimate, HIPAA covered entities and business associates should ask for the OCR complaint transaction number or the investigator's email address or ask for a confirmation email from the "investigator's" email address which will end in hhs.gov if it is legitimate. Report incidents of individuals posing as law enforcement to the FBI. Questions or concerns can be sent to OCRMail@hhs.gov.

***

1. ENFORCEMENT DISCRETION FOR COVID-19 TESTING SITES

OCR has issued a notice of enforcement discretion for COVID-19 Community-Based Testing Sites ("CBTS"). OCR will not impose penalties for noncompliance with HIPAA requirements against covered entities acting as health care providers and business associates that are participating in good faith in the operation of a CBTS. Retroactive to March 13, 2020, the enforcement discretion will remain effective until the Secretary of HHS declares a public health emergency no longer exists or the declared public health emergency (as extended) expires.

COVID-19 CBTS

A CBTS allows health care providers and their business associates to perform specimen collection and testing for COVID-19 only to the public whether through mobile, drive-through or walk-up sites.

Safeguards Encouraged but Not Required

OCR is still "encouraging" health care providers to implement reasonable safeguards to protect privacy and security, even though it will not enforce penalties against covered entities and business associates for failure to comply. Such safeguards include:

- Use and disclose only the minimum necessary PHI, unless for treatment purposes.
- Set up physical barriers to provide privacy during sample collection.
- Control traffic (pedestrian and vehicle) to create distance and minimize the ability of people to see or overhear screening interactions at a CBTS. The six-foot distance suggested to prevent the spread of COVID-19 is recommended.

- Create a buffer zone to prevent the public and/or media from viewing the site.
- Use secure technology to record and transmit ePHI.
- Post a Notice of Privacy Practices ("NPP") or instructions to find the online version of the NPP where individuals who approach the CBTS can see.

Practical Takeaways

Covered entities and business associates participating in the operation of COVID-19 CBTS should:

- Enact the safeguards listed above, as possible.
- Remember that not all covered entities are subject to this enforcement discretion – health plans or health care clearinghouses who are covered entities are not excused from compliance with HIPAA requirements when performing health plan and clearinghouse functions.

2. ENFORCEMENT DISCRETION FOR BUSINESS ASSOCIATE PUBLIC HEALTH DISCLOSURES

Under HIPAA, business associates are only allowed to use and disclose PHI for public health and health oversight purposes if the applicable business associate agreement ("BAA") expressly allows it or such disclosure is required by law. However, OCR has issued a notification of enforcement discretion for business associates who, in good faith, provide a covered entity's PHI to a health oversight agency for public health or health oversight activities during the COVID-19 pandemic or otherwise use or disclose such PHI in accordance with HIPAA's public health activities and health oversight activities provisions. This means that OCR will not impose penalties for such disclosure, *whether or not such use or disclosure is permitted under the BAA or the underlying agreement*. If a business associate makes a disclosure as permitted by this enforcement exception, the business associate must, within 10 days of making the disclosure (or the first of a series of uses or disclosures), provide notice to the covered entity.

In responding to the COVID-19 pandemic, entities like public health authorities and health oversight agencies, health departments and state emergency operations centers had sought PHI from business associates or requested analytics of PHI from business associates to help ensure the public's health and safety. Several of these public health and oversight entities had their requests denied or delayed by business associates that expressed concern that they were not permitted to share PHI for this purpose pursuant to the BAAs with their covered entity clients.

Uses and Disclosures Covered by This Notice

As a result of this enforcement exception, business associates are permitted to use and disclose PHI without amending the BAA between the business associate and covered entity:

- In assisting the CDC or similar state authority to prevent or control the spread of COVID-19; or
- CMS or similar state oversight agency for purposes of overseeing and providing assistance with COVID-19 response.

Business associates remain responsible to safeguard information shared in accordance with the Security Rule and to notify covered entities of any breaches of unsecured PHI.

To the extent a use or disclosure for public health or health oversight activities is required by law, rather than simply permitted, or is already expressly permitted in the BAA, business associates can continue to use and disclose PHI in accordance with such legal requirements and contractual allowances without relying on this new enforcement exception or providing notice to the covered entity within 10 days. This enforcement exception appears to only apply to legally permitted disclosures for public health and health oversight activities that are not contemplated by the BAA with the covered entity.

This enforcement discretion also extends to the covered entities whose PHI is disclosed by the business associates for such purposes. It is effective until the Secretary declares that the public health emergency no longer exists or upon the expiration date of the declared public health emergency, whichever occurs first.

Next Steps for Business Associates and Covered Entities

Business associates must note that this exercise of enforcement discretion only applies to OCR issuing penalties under the HIPAA Privacy

Rule. It does not address other state or federal laws, including those related to breach of contract claims. Business associates who violate the terms of a BAA may still face claims from the covered entity that the business associate breached the contract. Further, the business associate is not excused for violations of the HIPAA Security Rule. Business associates may elect to proactively reach out to the covered entity's privacy officer before responding to a request from a public health or health oversight entity, so the parties can agree to a waiver of the terms of the BAA with respect to this type of use or disclosure of PHI. Business associates must ensure any transfer of PHI is done in accordance with the HIPAA Security Rule. Business associates should assess:

1. Whether any more stringent laws apply to the information and prohibit the release; and
2. Whether their contracts with covered entity clients contain other confidentiality obligations that require a waiver prior to the release of information for these public health and health oversight activities

To qualify for this OCR enforcement discretion, a business associate must:

1. Make a good faith use or disclosure of PHI for public health activities or health oversight activities consistent with HIPAA requirements;
2. Inform the covered entity within 10 calendar days after the use or disclosure. OCR also notes that, alternatively, the covered entity can be informed the date the sharing commences, which implies that ongoing uses and disclosures for these purposes would be considered permissible.

Covered entities may be uneasy with the idea of a business associate sharing unspecified PHI for these purposes before notifying the covered entity. Covered entities should consider proactively contacting their business associates who may receive requests of this nature to work out an acceptable approach to this use or disclosure of PHI.

3. DISCLOSURES TO LAW ENFORCEMENT, PARAMEDICS, FIRST RESPONDERS AND PUBLIC HEALTH AUTHORITIES

On March 24, 2020, OCR issued HIPAA guidance regarding disclosures to law enforcement, paramedics, other first responders and public health authorities in light of the COVID-19 pandemic. The guidance includes:

- **Sharing without Authorization**. Discussion points and examples to assist covered entities in understanding when the Privacy Rule permits them to share the name or other identifying information of an infected individual with such first responders and public health authorities without the individual's written authorization.
- **HIPAA Applicability**. The guidance again notes that HIPAA only applies to covered entities and their business associates. The guidance is not intended to imply that *all* public health authorities, 911 call centers, or prison doctors, for example, are subject to HIPAA.
- **Sharing Permitted by HIPAA**. The guidance clarifies the regulatory permissions that covered entities may use to disclose PHI to first responders and others so they can take extra precautions or use personal protective equipment, including the following:
  - **Treatment**. When needed to provide treatment, for example during a patient's transport from one facility to another;
  - **Required by Law**. When required by law, such as when required to report confirmed or suspected cases to public health authorities;
  - **Preventing/Controlling Disease**. When otherwise notifying public health authorities in order to prevent or control the spread of disease;
  - **Exposures**. When first responders may be at risk for an infection due to exposure or otherwise at risk for contracting or spreading the disease, in accordance with state laws authorizing the notification of persons as necessary to conduct a public health intervention or investigation; and
  - **Serious and Imminent Threat**. When disclosure is necessary to prevent or lessen a serious and imminent threat to the health and safety of a person or the public, to someone able to prevent or lessen the threat.
    - For example, HIPAA permits a covered entity, consistent with applicable law and standards of ethical conduct, to disclose PHI about individuals who have tested positive for COVID-19 to fire department personnel, child welfare workers, mental health crisis services personnel, or others charged with protecting the health or safety of the public if the covered entity believes in good faith that the disclosure of the information is necessary to prevent or minimize the threat of imminent exposure to such personnel in

the discharge of their duties.

- **Law Enforcement/Jails**. When responding to a request for PHI by a correctional institution or law enforcement official having lawful custody of an inmate or other individual, if necessary to provide care to the individual, to protect the health and safety of others transferring, transporting or in contact with the individual at the facility, including to identify persons who may have been exposed or to prevent the exposure of others.

Minimum Necessary. The guidance also includes a reminder that, generally, covered entities must make reasonable efforts to limit the PHI used or disclosed to that which is the "minimum necessary" to accomplish the purpose for the disclosure. Therefore, information should not be posted publicly, such as on a website or through distribution to the media, and lists should only be distributed to those in the best position to use them on a “per call” basis – such as to EMS dispatch or a 911 call center – not to every individual EMS provider or law enforcement officer.

4. OCR WILL NOT IMPOSE HIPAA PENALTIES FOR CERTAIN NONCOMPLIANT TELEHEALTH VISITS

Enforcement Discretion

- OCR will not impose penalties against covered health care providers for noncompliance with HIPAA's Privacy, Security, and Breach Notification Rules if such providers, in good faith, use non-public facing remote communications technologies to provide telehealth services in a manner that does not fully comply with HIPAA requirements. OCR has issued detailed guidance, as well.
- This means FaceTime, Google Hangouts video and Skype may be used during the public health emergency.
- This enforcement discretion only applies to covered entity health care providers that provide telehealth services. OCR emphasized that entities that only *pay* for telehealth services are not covered, such as a health insurance company that pays for such services.

Patients and Telehealth Services Covered

- This discretion applies to all health care services provided via telehealth technology, not just health care services related to COVID-19.
- The discretion applies to all patients receiving telehealth services, whether or not they received Medicare or Medicaid.

Business Associate Agreement Is Not Required

- A BAA is not required for agreements with vendors providing video communication technology for telehealth visits for the duration of the national emergency declaration.
- The covered health care provider could still ask the vendor to agree to safeguards that are similar to those found in a business associate agreement in order to have some assurance of security practices, if desired.

Vendors Claiming HIPAA Compliance

- Covered entity health care providers who wish to engage a vendor that will agree to comply with HIPAA requirements may consider the following vendors, who have been identified but not endorsed or evaluated by OCR:
  - Skype for Business
  - Updox
  - VSee
  - Zoom for Healthcare
  - doxy.me
  - Google G Suite Hangouts Meet

Recommended Steps

- Health care providers should:
  - Notify patients of the privacy and security risks of their telehealth visit.
  - Enable all available encryption and privacy modes when using the communications technology. Even if not punishable under HIPAA, security issues can disrupt telehealth visits. Certain vendors have experienced cybersecurity threats, and health care providers should carefully consider using insecure. For a deeper dive into security issues brought on by certain video-conferencing technologies, see our article here.
  - Terminate any vendors whose technologies do not comply with HIPAA when the national emergency declaration ceases unless the vendor has come into compliance and will agree to enter a business associate agreement.
  - **Do not use public-facing technology, such as Facebook Live, Twitch or TikTok. These interactions can be visible to the public, not just the participants in the communication.**
  - Be mindful that outside of this enforcement discretion, HIPAA continues to apply during the COVID-19 pandemic. Details about HIPAA compliance during the COVID-19 pandemic are available here.

Other Telehealth Privacy Considerations

- 42 CFR Part 2
  - For health care providers subject to 42 CFR Part 2 ("Part 2"), the Substance Abuse and Mental Health Services Administration ("SAMHSA"), issued guidance on sharing Part 2 records without patient consent in emergencies. Part 2 providers who treat patients with substance use disorders are having to provide services remotely, through telehealth or only telephonic means in response to COVID-19. Obtaining written patient consent to share Part 2 records may not be possible in these scenarios.
  - In the guidance, SAMHSA highlights the Part 2 medical emergency exception. This permits a Part 2 program to share Part 2 records without patient consent, when consent cannot be obtained, for purposes of a bona fide medical emergency, as determined by the professional judgment of the provider.
    - Historically, the definition of a "bona fide medical emergency" was interpreted as a significant *medical event*. This guidance implies that a health care provider might determine that a situation itself, such as inability to obtain care via means other than telehealth, could constitute a medical emergency.
  - While SAMHSA has not gone so far as to specifically state that consent requirements are waived, this is a helpful reminder that in the event of a bona fide emergency where patient consent to share Part 2 records cannot be obtained in writing, Part 2 providers can rely on the emergency exception, as determined necessary by the provider, as a mechanism to ensure patients receive necessary care.
  - SAMHSA notes in the guidance that as necessary, Part 2 records shared with the medical personnel treating the patient may be redisclosed by the medical personnel for treatment purposes.

- Recommendations
  - Part 2 providers must document any sharing of Part 2 records without consent in accordance with their Part 2 policies.
  - Although no business associate agreement is required to share Part 2 records with medical personnel in a bona fide medical emergency, if Part 2 records will be shared with a technology vendor and patient consent cannot be obtained, a "qualified service organization agreement" must be entered into. This requires an entity providing services to a Part 2 program to acknowledge that it will receive Part 2 patient records and be bound by Part 2 requirements, and will resist efforts to obtain access to Part 2 records, except as permitted by Part 2. The provisions required in the qualified service organization agreement may be incorporated into the business associate agreement entered into with the vendor.

Additional information about implementing telehealth services during the COVID-19 pandemic is available here.

5. HIPAA SECTION 1135 WAIVER

Waivers under Section 1135(b)(7) of the Social Security Act have been issued in response to the Coronavirus Pandemic, including a limited waiver of some HIPAA Privacy Rule requirements.

The HIPAA waiver only applies:

- To covered entities;
- In the designated geographic area; and
- During the first 72 hours after the activation of the entity's emergency response plan.

The HIPAA waiver only affects:

- *Communications about Patient.* Requirements to obtain a patient's agreement to speak with family members or friends or to honor a patient's request to opt-out of the facility directory (per 45 C.F.R. § 164.510);
- *Notice of Privacy Practices*. The requirement to distribute a notice of privacy practices (per 45 C.F.R. § 164.520); and
- *Confidential Communications and Right to Restrict.* The patient's right to request privacy restrictions or confidential communications (per 45 C.F.R. § 164.522).

If the limitations and scope of this waiver do not address specific difficulties arising from COVID-19, it may be possible to seek additional Section 1135 waiver requests to the CMS Regional Office.

Contact Melissa Markey if you have questions.

6. OCR BULLETIN: HIPAA AND COVID-19

In light of the Novel Coronavirus outbreak ("COVID-19"), the U.S. Department of Health and Human Services Office for Civil Rights ("OCR") recently issued a bulletin to remind HIPAA covered entities and their business associates that HIPAA Privacy Rule protections are not wholly set aside in an emergency. However, OCR also provided guidance on Privacy Rule exceptions that permit protected health information ("PHI") to be shared during emergency situations and infectious disease outbreaks, like COVID-19. These specific exceptions include:

1. Disclosures to treat a patient;
2. Disclosures to a public health authority;
3. Disclosures at the direction of a public health authority;
4. Disclosures to people who are at risk of contracting or spreading a disease;
5. Disclosures to those involved in a patient's care; and
6. Disclosures to prevent a serious and imminent threat.

Disclosures for Treatment - Covered entities may disclose PHI without patient authorization if the disclosure is "necessary to treat the patient or to treat a different patient." "Treatment" includes provider consultations, patient referrals for treatment and care coordination or management between health care providers.

Disclosures for Public Health Activities - PHI may also be disclosed, under certain circumstances, to public health authorities, to foreign government agencies at the direction of a public health authority and to persons at risk of contracting or spreading a disease or condition. A "public health authority" is an agency or authority of the United States government, a state, a territory, a political subdivision of a state or territory or Indian tribe that is responsible for public health matters as part of its official mandate, as well as a person or entity acting under a grant of authority from, or under a contract with, a public health agency. This would include entities such as the CDC or a state or local health department, that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury or disability. In cases of disclosure to persons at risk, the disclosure of PHI should be authorized by state law and be necessary to prevent or control the spread of the disease or otherwise to carry out public health interventions or investigations.

Disclosures to Those Involved in a Patient's Care - The Privacy Rule allows covered entities to disclose PHI to family, friends and others involved in an individual's care. PHI regarding a patient's location, condition or death may also be shared in order to locate, notify or identify family members or others responsible for a patient's care. Generally, verbal permission from the patient should be obtained. If verbal permission is unable to be obtained from a patient due to incapacity or unavailability, the information should only be shared if in the provider's professional judgment it is in that patient's best interest to do so.

A covered entity may also share PHI with disaster relief organizations, such as the American Red Cross, authorized by law or charter to assist in disaster relief efforts, in order to coordinate notification of family members or others involved in a patient's care.

Disclosures to Avert a Serious and Imminent Threat - Consistent with applicable law (such as state statutes, regulations or case law) and the provider's standards of ethical conduct, a covered entity may share patient information as necessary to prevent or lessen a serious and imminent threat to the health and safety of a person or the public with anyone in a position to lessen the serious and imminent threat. HIPAA defers to health care providers' professional judgment, regarding the nature and severity of the threat in decisions regarding disclosures of PHI for such health and safety purposes.

Generally Disclosures to Media and Public NOT Permissible - Except in very limited circumstances described in the bulletin, affirmative reporting to the media or the public at large about an identifiable patient or the disclosure to the public or media of specific information about the treatment of an identifiable patient, such as specific tests, test results or details of a patient's illness, may not be done without the patient's written authorization (or the written authorization of a personal representative who is a person legally authorized to make health care decisions for the patient).

Minimum Necessary Rule Still Applies - Generally, if a disclosure is to be made, covered entities must make a reasonable effort to limit the PHI so that only the minimum necessary information is disclosed. This "minimum necessary standard" is not required for disclosures to other covered entities and health care providers for the purpose of patient treatment. In situations where a public health authority, such as the CDC, requests PHI, covered entities may assume that the information requested by the public health authority is minimally necessary for its public health purposes.

Be Mindful of Safeguards - Finally, the OCR reiterates that both covered entities and their business associates must continue to implement and adhere to reasonable administrative, physical and technical safeguards in emergency situations to protect PHI from unlawful use or disclosure. Internally, covered entities should continue to apply their role-based access policies to limit access to PHI to only those workforce members who need it to carry out their duties and monitor for unauthorized or impermissible access.

If you have any questions or would like additional information about this topic, please contact:

- Mark Swearingen at (317) 977-1458 or mswearingen@hallrender.com;
- Melissa Markey at (248) 740-7505 or mmarkey@hallrender.com;
- Charise Frazier at (317) 977-1406 or cfrazier@hallrender.com;
- Stephane Fabus at (414) 721-0904 or sfabus@hallrender.com;
- Patricia Connelly at (317) 429-3654 or pconnelly@hallrender.com; or
- Your regular Hall Render attorney.

Please refer to Hall Render's COVID-19 resource center webpage and hotline at 317-429-3900 for any questions, as well as up-to-date information regarding the virus.

For more information on Hall Render's HIPAA, Privacy & Security services, click here.