FELDESMAN+TUCKER+LEIFER+FIDELL

1129 20th Street, NW
Suite 400
Washington, DC 20036

T. 202.466.8960
F. 202.293.8103
www.ftlf.com

CLIENT ALERT: Compliance with Federal Patient Confidentiality Laws and Regulations During and After COVID-19

To support health care providers during the COVID-19 public health emergency, the Department of Health and Human Services (HHS) has issued a variety of guidance on the application and enforcement of the federal laws and regulations related to patient confidentiality. HHS announced it will not enforce certain provisions of HIPAA during this period and it released COVID-19 specific guidance on permitted disclosures under both HIPAA and 42 CFR Part 2. Congress included significant amendments to these federal confidentiality laws and regulations in the recently signed CARES Act.

Below is a summary of the updates from HHS as of April 13th, as well as a brief summary of the CARES Act changes. Readers should review this information, along with underlying documents, to ensure compliance with the federal laws and regulations related to patient confidentiality[1] during and after the COVID-19 public health emergency.

HIPAA

The Office for Civil Rights (OCR) enforces the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security and Breach Notification Rules ("the HIPAA Rules").[2] Covered entities are required to comply with the HIPAA Rules. Covered entities include health care providers that transmit any information, such as claims, in an electronic form in connection with a transaction for which HHS has adopted a standard. If a covered entity engages with an individual or entity to provide a service or function that involves the disclosure of protected health information (PHI), the individual or entity is considered a business associate. The covered entity and business associate must execute a written business associate agreement or other arrangement that establishes what the business associate has been engaged to do and that requires the business associate to comply with the applicable HIPAA Rules.

---

[1] State and local laws and regulations may provide additional protections to patient records. Where a state law or regulation provides greater privacy protections or privacy rights, HIPAA covered entities and Part 2 programs must follow the state law or regulation. The guidance from HHS does not address the application and enforcement of state confidentiality laws or regulations.

[2] OCR also enforces the federal civil rights laws and conscious and religious freedom laws. OCR has released a Bulletin on the applications of these laws during the COVID-19 public health emergency, available at: https://www.hhs.gov/about/news/2020/03/28/ocr-issues-bulletin-on-civil-rights-laws-and-hipaa-flexibilities-that-apply-during-the-covid-19-emergency.html.

Over the past weeks, OCR has issued the following items:

- Limited Waiver of HIPAA Sanctions and Penalties During a Nationwide Public Health Emergency ("Limited Waiver"): On March 15th, HHS's Limited Waiver became effective. The Limited Waiver applies to any hospital that has instituted its disaster protocol. The Limited Waiver lasts for up to 72 hours from the time the disaster protocol is implemented. Under the Limited Waiver, HHS waives sanctions and penalties against a covered hospital for non-compliance with the following provisions of the HIPAA Privacy Rule:
    - Requirements to obtain a patient's agreement to speak with family members or friends involved in the patient's care
    - Requirement to honor a request to opt out of the facility directory
    - Requirement to distribute a notice of privacy practices
    - Patient's right to request privacy restrictions
    - Patient's right to request confidential communications

  Compliance Tip: The Limited Waiver applies only to hospitals; it does *not* apply to other covered entities.

- Notice of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency (Notice of Enforcement Discretion for Telehealth) and FAQ on Telehealth: On March 17th, OCR announced that it will temporarily waive potential HIPAA penalties for covered entities that serve patients through non-public communication technologies during the COVID-19 public health emergency. Under the Notice of Enforcement Discretion for Telehealth, covered entities may use non-public communication technologies, such as FaceTime, Skype and Zoom, *without* an executed BAA. Covered entities are prohibited from using public communication technologies, such as FaceBook Live, Twitch, and TikTok.

  Compliance Tip: While OCR's waiver of certain HIPAA penalties related to telehealth during the COVID-19 public health emergency currently provides flexibility, the enforcement waiver is temporary. Covered entities that have launched or expanded telehealth during this period should evaluate whether they will continue such services after the COVID-19 public health emergency and, if so, execute a business associate agreement with a HIPAA-compliant telehealth vendor. The Notice of Enforcement Discretion for Telehealth provides a list of vendors that have represented to OCR that they provide HIPAA-compliant video communication products and will sign a BAA. Covered entities that will discontinue telehealth after the COVID-19 public health emergency should develop a communication plan to inform patients and staff members, determine whether any exceptions will be permitted and create an internal monitoring process to ensure use of the video and texting platforms is discontinued.

- COVID-19 and HIPAA Disclosures to Law Enforcement, Paramedics and Other First Responders and Public Health Authorities (COVID-19 Disclosure Guidance): The HIPAA Privacy Rule permits covered entities to disclose PHI without a patient's consent or authorization for certain purposes, including for public health activities and to notify anyone in a position to prevent or lessen a serious and imminent threat. The COVID-19 Disclosure Guidance clarifies that, when authorized by law, a covered entity may disclose PHI to a first responder at risk of infection because they have been exposed to COVID-19 or who may otherwise be at risk of contracting or spreading COVID-19. The COVID-19 Disclosure Guidance also clarifies that a covered entity may disclose PHI to first responders when disclosure is necessary to prevent or lessen a serious and imminent threat to the health and safety of a person or the public.

  Compliance Tip: Covered entities should identify their public health reporting obligations under state and local laws and regulations, as those requirements will guide decision-making related to disclosure of COVID-19-related patient information. For example, state laws typically authorize state or local public health departments to collect PHI to prevent or control disease. HIPAA permits a covered entity to disclose PHI to such public health departments as described in the state's law. For example, a covered entity may be required to report positive COVID-19 test results to the Department of Public Health under the state's public health regulations. HIPAA also permits the state or local public health department, in accordance with state law, to disclose PHI to a police officer or other persons who may come in contact with a person who tested positive for COVID-19 for purposes of preventing or controlling the spread of COVID-19.

- Notice of Enforcement Discretion under HIPAA to Allow Uses and Disclosures of Protected Health Information by Business Associates for Public Health and Health Oversight Activities in Response to COVID-19: On April 2nd, OCR announced that it will temporarily waive potential HIPAA penalties for covered entities and business associates when a business associate uses or discloses PHI for public health and health oversight activities during the COVID-19 nationwide public health emergency. Where a business associate would usually only be permitted to use and disclose PHI as permitted under a business associate agreement (or other written agreement/arrangement), or as required by law, under the Notice of Enforcement Discretion for Business Associates, OCR will waive potential HIPAA penalties if the business associate makes a good faith use or disclosure of PHI for public health activities (45 CFR 164.512(b)) or for health oversight activities (42 CFR 164.512(d)). Within ten calendar days the business associate must inform the covered entity of the use or disclosure.

  Compliance Tip: Covered entities should ensure that information about a business associate's disclosures for public health or health oversight activities are documented in the patient's record as records of such disclosures must be

available to a patient requesting an accounting of disclosures under 45 CFR 164.528.

- Notice of Enforcement Discretion Regarding COVID-19 Community-Based Testing Sites (CBTS) During the COVID-19 Nationwide Public Health Emergency: On April 9th, OCR announced that it will temporarily waive potential HIPAA penalties against covered health care providers or their business associates in connection with the good faith participation in the operation of COVID-19 CBTS. The waiver is retroactive to March 13th. It applies to certain covered health care providers, including large pharmacy chains, and their business associates which participate in the operation of mobile, drive-through or walk-up sites that provide only COVID-19 specimen collection and testing services to the public. OCR states that potential HIPAA penalties still apply to all other HIPAA-covered operations of the covered health care provider or business associate, unless otherwise stated by OCR. Covered health care providers are also encouraged to implement reasonable safeguards related to the operation of COVID-19 CBTS.

  Compliance Tip: Covered entities should ensure they understand the scope of any applicable waiver and maintain compliance with the applicable HIPAA Rules for activities and operations not covered by the waiver. When possible, covered entities should implement reasonable safeguards for activities and operations covered by the waiver.

OCR's HIPAA, Civil Rights and COVID-19 webpage includes the documents discussed here and is regularly updated by OCR. Covered entities should check OCR's webpage for updated and new items and monitor the information sent through the OCR Privacy and Security Listserv.

SAMHSA

The Substance Abuse and Mental Health Services Administration (SAMHSA) has the statutory authority to promulgate the federal regulations governing the Confidentiality of Substance Use Disorder Patient Records (42 CFR Part 2 ("Part 2")). The Part 2 regulations apply to "Part 2 programs" (42 CFR 2.11) and lawful holders of Part 2-protected information. Part 2 restricts the disclosure of any information identifying a patient as having or having had a SUD either directly, by reference to publicly available information, or through verification of such identification. A patient's written consent to disclose Part 2-protected information is required unless one of the narrow exceptions applies.

In March, SAMHSA issued the following guidance:

- COVID-19 Public Health Emergency Response and 42 CFR Part 2 Guidance: On March 19th, SAMHSA issued a guidance document on the use and

disclosure of Part 2-protected information during the COVID-19 pandemic. The guidance emphasizes that, under the medical emergency exception at 42 CFR 2.51, a Part 2 program or lawful holder may disclose Part 2-protected information without a patient's consent if the provider determines a bona fide medical emergency exists for purpose of providing needed treatment to patients.

Compliance Tip: Under the medical emergency exception, Part 2-protected information may *only* be disclosed to medical personnel; each disclosure must be immediately documented as described under 42 CFR 2.51(c); and the amount of information disclosed must be limited to the information necessary to carry out the purpose of the disclosure per 42 CFR 2.13(a).

SAMHSA established a Coronavirus (COVID-19) webpage where the Part 2 guidance is posted.

The CARES Act

The Coronavirus Aid, Relief, and Economic Security ("CARES") Act includes significant amendments to the federal law on the confidentiality of substance use disorder records (42 USC 290dd-2) and requires the Secretary of HHS to revise both the Part 2 and HIPAA regulations in the coming year. Below is a summary of the key amendments under the CARES Act:

1. Consent: After signing an initial written consent, a patient's Part 2-protected records may be used or disclosed by a Part 2 Program, covered entity or business associate for the purposes of treatment, payment and health care operations[3] as permitted by the HIPAA Rules. A patient's written consent may be given once for such future uses and disclosures, until the patients revokes their consent in writing. Patients may request an accounting of disclosures and request restrictions on the use and disclosure of their information, as permitted by the HIPAA Rules.
2. Disclosures to Public Health Authorities: De-identified information may be disclosed to public health authorities. Such information must meet the standards under 45 CFR §164.514(b) which require either: (1) an appropriately knowledgeable and experienced individual apply generally accepted statistical and scientific principles and methods to determine (and document) that the risk of reidentification is very small; or (2) the covered entity to remove the 18 identifiers listed at 45 CFR §164.514(b)(2)(i) and to have no actual knowledge that reidentification of the patient information is possible.

[3]The definition of health care operations shall *not* include creating de-identified health information or a limited data set, or fundraising.

3. Disclosures in Criminal, Civil or Administrative Investigations, Actions or Proceedings: Disclosure of Part 2-protected records or testimony relaying information in such records for criminal, civil or administrative investigations, actions or proceedings may only be authorized by a court order or with the consent of the patient.
4. Antidiscrimination: Entities are prohibited from discriminating against an individual on the basis of Part 2-protected information received either intentionally or inadvertently in providing or providing access to health care, employment and worker's compensation, housing, courts, or social services and benefits provided by federal, state or local governments.
5. Breaches: The HIPAA breach notification requirements and penalties apply to breaches of Part 2-protected information.

The CARES Act states that the Secretary of HHS is to revise the regulations to apply to uses and disclosures of Part 2-protected information on or after March 27th, 2021 (12 months after the enactment of the CARES Act) and update the HIPAA notice of privacy practices requirements by no later than March 27th, 2021 (one year after the enactment of the CARES Act). It is unclear whether the regulations required by the CARES Act will be released along with the other changes to Part 2 and HIPAA expected this year.[4]

Frequently Asked Questions

1. **Does the Notice of Enforcement Discretion for Telehealth only apply to COVID-19 screening and care?**

   No. The Notice of Enforcement Discretion for Telehealth applies to use of non-public communication technologies to assess or treat any condition that a covered health care provider believes, in their professional judgement, can be provided through telehealth, including providing psychological evaluations and mental health counseling.

2. **Given the recent news reports about the security of Zoom, is it still permissible to use Zoom to provide telehealth services?**

   As of April 13th, Zoom is still listed in OCR's Notice of Enforcement Discretion for Telehealth as one of the popular applications for video chats that covered entities may use to provide telehealth during the COVID-19 public health emergency without risk that OCR might seek to impose a penalty for non-

[4] For more on the expected changes to Part 2, *see* "SAMHSA Proposes Changes to 42 CFR Part 2" (posted September 16, 2019), available at https://www.feldesmantucker.com/samhsa-proposes-changes-to-42-cfr-part-2/. For more on the expected changes to HIPAA, *see* "OCR Requests Information on Revising HIPAA Rules" (posted February 5, 2019), available at https://www.feldesmantucker.com/ocr-requests-information-on-revising-hipaa-rules/.

compliance with the HIPAA Rules. OCR encourages covered entities to enable all available encryption and privacy modes when using any non-public communication technology. For covered entities seeking additional privacy protections for telehealth, OCR recommends covered entities engage with a HIPAA-compliant technology vendor that will enter into a business associate agreement. According to the Notice of Enforcement Discretion for Telehealth, Zoom for Healthcare has represented to OCR that they will provide HIPAA-compliant video communication products and will enter into a business associate agreement.

3. **How will OCR notify covered entities that it is beginning to enforce the business associate requirements for telehealth?**

   OCR has stated that it will issue a notice to the public when it is no longer exercising its enforcement discretion. Covered entities should monitor OCR's HIPAA, Civil Rights and COVID-19 webpage and sign up for the OCR Privacy and Security Listserv.

4. **Will there be a period of time after the COVID-19 public health emergency ends in which covered entities can continue to use non-public communication technologies without penalties while they identify a HIPAA-compliant telehealth vendor?**

   OCR has not addressed this question in its guidance documents. Covered entities wanting to continue with telehealth after the COVID-19 public health emergency should identify a HIPAA-compliant telehealth vendor and execute a business associate agreement to ensure that patients have seamless telehealth access after the COVID-19 public health emergency.

5. **Our understanding is that the CARES Act aligns 42 CFR Part 2 SUD Treatment Confidentiality standards with HIPAA. What does that mean?**

   As described above, the amendments included in the CARES Act change the consent requirements such that after a patient's initial written consent, their Part 2-protected records may be used or disclosed for the purposes of treatment, payment and health care operations as permitted by the HIPAA Rules. This change will decrease the number of times a patient must consent in writing to the disclosure of their Part 2-protected records. SAMHSA's revised Part 2 regulations (expected in the next year) should provide additional detail on the consent requirements and process.

Questions? If you have questions about this information, please contact Dianne K. Pledgie, a Partner and a member of the health care compliance practice at Feldesman Tucker Leifer Fidell LLP, by e-mail at dpledgie@ftlf.com.