Thank you for joining us today. The webinar will begin shortly.

**Patient Confidentiality and COVID-19**

Operating the Navigation Panel

- **Presentation Slides**: Click the arrow on the handouts tab and then the document icon.
- **Questions**: Click the arrow on the questions tab, enter your question in the text box, and click ‘Send’
Patient Confidentiality and COVID-19

Molly S. Evans
Dianne K. Pledgie

March 27, 2020
This training has been prepared by the attorneys of Feldesman Tucker Leifer Fidell LLP. The opinions expressed in these materials are solely their views and not necessarily the views of any other individual, entity or organization.

The materials are being issued with the understanding that the authors are not engaged in rendering legal or other professional services. **If legal advice or other expert assistance is required, the services of a competent professional should be sought.**
• Partner at Feldesman Tucker Leifer Fidell LLP.
• Practices in areas of nonprofit law, corporate and business law, and health care law.
• Focus on assisting non-profits with regulatory, transactional, and corporate compliance matters including employment law.
• Ms. Evans was formerly in-house counsel at a large, multi-site non-profit in Washington, D.C. where she was responsible for identifying and managing legal risk issues.

Contact Information:
mevans@ftlf.com
202.466.8960
• Partner and Compliance Counsel at Feldesman Tucker Leifer Fidell LLP, specializing in, among other things, assisting health centers with the implementation of effective Compliance Programs.

• Manages the FTLF Premium Plan, Toolkit resources, monthly compliance webinars, and health center compliance news.

• Well-versed in the compliance issues facing health centers because of her experience as Chief Compliance Officer and Manager of Government Grants for Boston Health Care for the Homeless Program, one of the largest health center programs in the country.

Contact information: dpledgie@ftlf.com
202.466.8960
AGENDA

• Review recent information from the Office for Civil Rights (OCR) on HIPAA, including:
  – Limited Waiver
  – Notice of Enforcement Discretion
  – FAQ on HIPAA and Telehealth

• Review recent information from Substance Abuse and Mental Health Services Administration (SAMHSA) on 42 CFR Part 2 (Part 2), including:
  – Guidance on Medical Emergencies
HIPAA: General Rules and COVID-19 Specific Guidance, Waivers and Notices
HIPAA AND PERMITTED DISCLOSURES: GENERAL RULES

Sharing Patient Information Under HIPAA: General Rules

• **Treatment**
• Public Health Activities
• Disclosures to Family, Friends, and Others Involved in an Individual’s Care and for Notification
• Disclosures to Prevent a Serious and Imminent Threat
• Disclosures to Media and Others Not Involved in the Care of the Patient/Notification
• Minimum Necessary
Sharing Patient Information Under HIPAA: General Rules

Treatment

- Under the Privacy Rule, covered entities may disclose, **without a patient’s authorization**, protected health information about the patient as necessary to treat the patient or to treat a different patient.
- Treatment includes the **coordination** or **management** of health care and related services by one or more health care providers and others, **consultation** between providers, and the **referral** of patients for treatment.
COVID-19 and HIPAA: Disclosures to law enforcement, paramedics, other first responders and public health authorities

The HIPAA Privacy Rule permits a covered entity to disclose the protected health information (PHI) of an individual who has been infected with, or exposed to, COVID-19, with law enforcement, paramedics, other first responders, and public health authorities without the individual’s HIPAA authorization, in certain circumstances, including the following:

When the disclosure is needed to provide treatment. For example, HIPAA permits a covered skilled nursing facility to disclose PHI about an individual who has COVID-19 to emergency medical transport personnel who will provide treatment while transporting the individual to a hospital’s emergency department.
HIPAA AND PERMITTED DISCLOSURES: GENERAL RULES

Sharing Patient Information Under HIPAA: General Rules

Public Health Activities

• The HIPAA Privacy Rule recognizes the legitimate need for public health authorities and others responsible for ensuring public health and safety to have access to PHI that is necessary to carry out their public health mission. Therefore, the Privacy Rule permits covered entities to disclose needed PHI without individual authorization to:
  – a public health authority
  – at the direction of a public health authority, to a foreign government agency
  – to persons at risk
COVID-19 and HIPAA: Disclosures to law enforcement, paramedics, other first responders and public health authorities

- **When such notification is required by law.** For example, HIPAA permits a covered entity, such as a hospital, to disclose PHI about an individual who tests positive for COVID-19 in *accordance with a state law requiring the reporting* of confirmed or suspected cases of infectious disease to *public health officials*.

- **To notify a public health authority** in order to *prevent or control spread of disease*. For example, HIPAA permits a covered entity to disclose PHI to the CDC.

- **To a first responder** who may have been exposed to COVID-19 or may otherwise be at risk of contracting or spreading COVID-19, *if the covered entity is authorized by law*, such as state law, to notify persons as necessary in the conduct of a public health intervention or investigation.
Sharing Patient Information Under HIPAA: General Rules

Disclosures to Family, Friends, and Others Involved in an Individual’s Care and for Notification

• A covered entity may share PHI with a patient’s family members, relatives, friends, or other persons identified by the patient as involved in the patient’s care.

• A covered entity also may share information about a patient as necessary to identify, locate, and notify family members, guardians, or anyone else responsible for the patient’s care, of the patient’s location, general condition, or death. This may include, where necessary to notify family members and others, the police, the press, or the public at large.
Sharing Patient Information Under HIPAA: General Rules

Disclosures to Family, Friends, and Others Involved in an Individual’s Care and for Notification (continued)

• The covered entity should get verbal permission from individuals or otherwise be able to reasonably infer that the patient does not object, when possible; if the individual is incapacitated or not available, covered entities may share information for these purposes if, in their professional judgment, doing so is in the patient’s best interest.

• For patients who are unconscious or incapacitated: A health care provider may share relevant information about the patient with family, friends, or others involved in the patient’s care or payment for care, if the health care provider determines, based on professional judgment, that doing so is in the best interests of the patient.
Sharing Patient Information Under HIPAA: General Rules

Disclosures to Family, Friends, and Others Involved in an Individual’s Care and for Notification (continued)

A covered entity may share PHI with disaster relief organizations that, like the American Red Cross, are authorized by law or by their charters to assist in disaster relief efforts, for the purpose of coordinating the notification of family members or other persons involved in the patient’s care, of the patient’s location, general condition, or death. It is unnecessary to obtain a patient’s permission to share the information in this situation if doing so would interfere with the organization’s ability to respond to the emergency.
Sharing Patient Information Under HIPAA: General Rules

Disclosures to Prevent a Serious and Imminent Threat

- Health care providers may share patient information with anyone as necessary to prevent or lessen a serious and imminent threat to the health and safety of a person or the public – consistent with applicable law (such as state statutes, regulations, or case law) and the provider’s standards of ethical conduct.

- Thus, providers may disclose a patient’s health information to anyone who is in a position to prevent or lesson the serious and imminent threat, including family, friends, caregivers, and law enforcement without a patient’s permission. HIPAA expressly defers to the professional judgment of health professionals in making determinations about the nature and severity of the threat to health and safety.
COVID-19 and HIPAA: Disclosures to law enforcement, paramedics, other first responders and public health authorities

- A covered entity may disclose PHI to prevent or lessen a serious and imminent threat to a person or the public, **when such disclosure is made to someone they believe can prevent or lessen the threat, which may include the target of the threat.**

- For example, 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.**
Sharing Patient Information Under HIPAA: General Rules
Disclosures to Media and Others Not Involved in the Care of the Patient/Notification

• In general, except in the limited circumstances described elsewhere in this 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 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).
Sharing Patient Information Under HIPAA: General Rules

Disclosures to Media and Others Not Involved in the Care of the Patient/Notification (continued)

• Where a patient has not objected to or restricted the release of protected health information, a covered hospital or other health care facility may, upon a request to disclose information about a particular patient asked for by name, release limited facility directory information to acknowledge an individual is a patient at the facility, and may provide basic information about the patient’s condition in general terms (e.g., critical or stable, deceased, or treated and released).

• Covered entities may also disclose information when the patient is incapacitated, if the disclosure is believed to be in the best interest of the patient and is consistent with any prior expressed preferences of the patient.
Sharing Patient Information Under HIPAA: General Rules

Minimum Necessary

• For most disclosures, a covered entity must make reasonable efforts to limit the information disclosed to that which is the “minimum necessary” to accomplish the purpose. (Minimum necessary requirements do not apply to disclosures to health care providers for treatment purposes.)

• Covered entities may rely on representations from a public health authority or other public official that the requested information is the minimum necessary for the purpose, when that reliance is reasonable under the circumstances.
COVID-19 and HIPAA: Disclosures to law enforcement, paramedics, other first responders and public health authorities

A covered entity, such as a hospital, may provide a list of the names and addresses of all individuals it knows to have tested positive, or received treatment, for COVID-19 to an EMS dispatch for use on a per-call basis. The EMS dispatch (even if it is a covered entity) would be allowed to use information on the list to inform EMS personnel who are responding to any particular emergency call so that they can take extra precautions or use personal protective equipment (PPE).
COVID-19 and HIPAA: Disclosures to law enforcement, paramedics, other first responders and public health authorities

**NOTE:** Under this example, a covered entity should not post the contents of such a list publicly, such as on a website or through distribution to the media. A covered entity under this example also should not distribute compiled lists of individuals to EMS personnel, and instead should disclose only an individual’s information on a per-call basis. Sharing the lists or disclosing the contents publicly would not ordinarily constitute the minimum necessary to accomplish the purpose of the disclosure (*i.e.*, protecting the health and safety of the first responders from infectious disease for each particular call).
COVID-19 and HIPAA: Disclosures to law enforcement, paramedics, other first responders and public health authorities

A 911 call center may ask screening questions of all callers, for example, their temperature, or whether they have a cough or difficulty breathing, to identify potential cases of COVID-19. To the extent that the call center may be a HIPAA covered entity, the call center is permitted to inform a police officer being dispatched to the scene of the name, address, and screening results of the persons who may be encountered so that the officer can take extra precautions or use PPE to lessen the officer’s risk of exposure to COVID-19, even if the subject of the dispatch is for a non-medical situation.
COVID-19 and HIPAA: Disclosures to law enforcement, paramedics, other first responders and public health authorities

NOTE: A 911 call center that is a covered entity should only disclose the minimum amount of information that the officer needs to take appropriate precautions to minimize the risk of exposure. Depending on the circumstances, the minimum necessary PHI may include, for example, an individual’s name and the result of the screening. Covered entities should consult other applicable laws (e.g., state and local statutes and regulations) in their jurisdiction prior to using or making disclosures of individuals’ PHI, as such laws may place further restrictions on disclosures that are permitted by HIPAA.
HIPAA AND COVID-19: LIMITED WAIVER OF HIPAA PRIVACY RULE

Effective March 15th, sanctions and penalties are waived against covered hospitals that do not comply with certain provisions of the HIPAA Privacy Rule, including:

• Requirements to obtain a patient’s agreement to speak with family members or friends involved in the patient’s care under 45 CFR § 164.510(b)
• Requirement to honor a request to opt out of the facility directory under 45 CFR § 164.510(a)
• Requirement to distribute a notice of privacy practices under 45 CFR § 164.520
• Patient’s right to request privacy restrictions under 45 CFR § 164.522(a)
• Patient’s right to request confidential communications under 45 CFR § 164.522(b)
The waiver, issued by the Secretary of HHS, applies only:

1. In the **emergency area identified** in the public health emergency declaration;

2. To **hospitals** that have instituted a disaster protocol; and

3. For **up to 72 hours** from the time the hospital implements its disaster protocol.
The HIPAA Rules require that covered entities obtain satisfactory assurances from its business associate that the business associate will appropriately safeguard the protected health information it receives or creates on behalf of the covered entity. The **satisfactory assurances must be in writing**, whether in the form of a contract or other agreement between the covered entity and the business associate.
On March 17th, OCR issued a Notice of Enforcement Discretion and announced that it will not impose penalties against covered health care providers for the lack of a business associate agreement with any non-public facing remote communication product or any other noncompliance with the HIPAA Rules that relates to the good faith provision of telehealth services during the COVID-19 nationwide public health emergency.
Non-public facing remote communication products:

- As a default, allow only the intended parties to participate in the communication
- Employ end-to-end encryption
- Support individual user accounts, logins and passcodes
- Allow some degree of control over video or audio capabilities
Non-public facing remote communication platforms that **may be used**:

- Apple FaceTime
- Facebook Messenger video chat
- Google Hangouts video
- WhatsApp video chat
- Skype

And texting applications such as:

- Signal
- Jabber
- Facebook Messenger
- Google Hangouts
- WhatsApp
- iMessage
HIPAA AND COVID-19: OCR NOTICE ON TELEHEALTH

Public facing video communication products are designed to be open to the public or allow wide or indiscriminate access to the communication.

Public facing products that **should not be used** to provide telehealth services include:

- Facebook Live
- Twitch
- TikTok
- Other similar public facing remote communication products (chat rooms like Slack)
Applies to telehealth provided for any reason, including:

- Diagnosis and treatment of health conditions related to COVID-19
- Sprained ankle
- Dental consultation
- Psychological evaluation
- Review of physical therapy practices
- Adjustment of prescriptions
- Mental health counseling
OCR encourages covered entities to:

• Notify patients that the third-party applications potentially introduce privacy risks

• Enable all available encryption and privacy modes when using such applications

• Use a private location to conduct telehealth; encourage patients to use a private location to receive telehealth services
HIPAA AND COVID-19: RESOURCES

  - Includes links to:
    - February 2020 HIPAA and Novel Coronavirus
    - March 2020 HIPAA and COVID-19 Bulletin
    - Notice of Enforcement Discretion for Telehealth
    - FAQs on HIPAA and Telehealth
    - Disclosures of PHI to Law Enforcement, Paramedics, Other First Responders and Public Health Authorities
- Sign Up for the OCR Privacy and Security Listserv: https://www.hhs.gov/hipaa/for-professionals/listserv/index.html
Part 2: General Rules and COVID-19 Guidance
PART 2 AND DISCLOSURES: GENERAL RULES

The part 2 underlying statute, 42 U.S.C. 290dd–2, and this rule require a written patient consent to disclose part 2 information unless the disclosure is otherwise permitted under the part 2 statute or regulations. The statute, for instance, does not provide a general exception to the consent requirement for the purpose of sharing information with public health officials. In certain circumstances, disclosures of part 2 information may be authorized by court order to protect against an existing threat to life or of serious bodily injury (see § 2.63, Confidential communications) or to the extent necessary to meet a bona fide medical emergency in which the patient’s prior informed consent cannot be obtained (see § 2.51, Medical emergencies).

82 Fed. Reg. 6079
On March 19th SAMHSA issued a COVID-19 Guidance acknowledging:

“...there has been an increased need for telehealth services, and in some areas without adequate telehealth technology, providers are offering telephonic consultations to patients. In such instances, providers may not be able to obtain written patient consent for disclosure of substance use disorder records...”
PART 2 AND QUALIFIED SERVICE ORGANIZATIONS:
GENERAL RULES

42 CFR § 2.11: Qualified service organization (QSO) means an individual or entity who:

1. Provides services to a Part 2 program, and
2. Has entered into a written agreement (QSOA) with a Part 2 program under which that individual or entity:
   1. Acknowledges that in receiving, storing, processing, or otherwise dealing with any patient records from the Part 2 program, it is fully bound by Part 2; and
   2. If necessary, will resist in judicial proceedings any efforts to obtain access to patient identifying information related to substance use disorder diagnosis, treatment, or referral for treatment except as permitted by Part 2.
“The prohibitions on use and disclosure of patient identifying information under 42 C.F.R. Part 2 would not apply in these situations to the extent that, as determined by the provider(s), a medical emergency exists. Under 42 U.S.C. § 290dd-2(b)(2)(A) and 42 C.F.R. § 2.51, patient identifying information may be disclosed by a part 2 program or other lawful holder to medical personnel, without patient consent, to the extent necessary to meet a bona fide medical emergency in which the patient’s prior informed consent cannot be obtained. Information disclosed to the medical personnel who are treating such a medical emergency may be re-disclosed by such personnel for treatment purposes as needed....”
“....We emphasize that, under the medical emergency exception, providers make their own determinations whether a bona fide medical emergency exists for purposes of providing needed treatment to patients.”

In comments to the 2017 Final Rule, SAMHSA clarified:

• Any health care provider who is treating the patient for a medical emergency can make the determination (not limited to treating provider)

• The amount of information to be disclosed “must be limited to that information which is necessary to carry out the purpose of the disclosure” (per § 2.13(a))
“...We note that Part 2 requires programs to **document certain information in their records after a disclosure is made pursuant to the medical emergency exception.**”

42 CFR § 2.51(c)

Immediately following disclosure, the part 2 program shall document, in writing, the disclosure in the patient’s records, including:

1. The name of the medical personnel to whom disclosure was made and their affiliation with any health care facility;
2. The name of the individual making the disclosure;
3. The date and time of the disclosure; and
4. The nature of the emergency (or error, if the report was to FDA).
Proposed rule would amend 42 CFR § 2.51 to permit patient identifying information to be disclosed to **medical personnel** to the extent necessary to...

(2) **Meet a bona fide medical emergency in which a part 2 program is closed** and unable to provide services or obtain the prior written consent of the patient, during a temporary **state of emergency declared by a state and/or federal authority as the result of a natural or major disaster**, until such time that the part 2 program resumes operations.
PART 2 AND COVID-19: RESOURCES

- https://www.samhsa.gov/coronavirus
Molly S. Evans
MEvans@FTLF.com
202-466-8960

Dianne K. Pledgie
Dpledgie@FTLF.com
202-466-8960

Feldesman Tucker Leifer Fidell LLP
(202) 466-8960 (Reception)
(855) 200-3822 (Training Team)
www.ftlf.com
Learning.ftlf.com
UPCOMING LIVE WEBINARS & VIRTUAL RESOURCES

<table>
<thead>
<tr>
<th>Upcoming Live Webinars</th>
<th>2020 Compliance Manual Webinar Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>March 30&lt;sup&gt;th&lt;/sup&gt;</td>
<td>Part IV: Emergency Preparedness for Longterm Care Facilities (Pot-Acute Care in 2020 Series)</td>
</tr>
<tr>
<td>April 9&lt;sup&gt;th&lt;/sup&gt;</td>
<td>Opioid Epidemic: Enforcement Updates</td>
</tr>
<tr>
<td>May 14&lt;sup&gt;th&lt;/sup&gt;</td>
<td>PACE and Health Centers – Key Opportunities and Risk Areas</td>
</tr>
<tr>
<td>June 18&lt;sup&gt;th&lt;/sup&gt;</td>
<td>Top Ten Tips for OSV Prep</td>
</tr>
<tr>
<td>July 23&lt;sup&gt;rd&lt;/sup&gt;</td>
<td>Preventing and Responding to Workplace Violence: A Risk Management Approach</td>
</tr>
</tbody>
</table>

All webinars start @ 1 pm ET unless otherwise noted.

Premium Plan Membership

Our annual subscription containing all the necessary tools to develop, implement, and/or improve your Compliance Program.

What’s Included?
- Monthly Compliance Webinars
- Toolkits - Seven Elements of a Compliance Program, Section 330 Health Center Program & Confidentiality for Health Centers
- Advice Lines – Compliance Officer, HIPAA Privacy, & FTCA

For more information and to register:
Email learning@ftlf.com or go to https://learning.ftlf.com