NATIONAL ASSOCIATION OF Community Health Centers®

Resource Packet
Patient Confidentiality and Telehealth Guidance
Issued September 2020

Health centers are serving on the frontline, providing critical health care services in communities dealing with the coronavirus and COVID-19. This packet contains guidance on immediate and long-term telehealth/patient confidentiality questions relevant to federally qualified health centers (FQHCs) across the country. The resources contained within aim to provide risk management considerations for a sustainable telehealth program.

The enclosed guidance is current as of the issuance date and may require revisions as circumstances evolve in our rapidly changing operating environment.

Enclosed

Additional Resources

For additional resources on Telehealth generally, please see the Health Center Resources Clearinghouse (www.healthcenterinfo.org).

Disclaimers

These materials have been prepared by the attorneys of Feldesman Tucker Leifer Fidell LLP. The opinions expressed in these materials are solely their views and do not necessarily represent the opinions of the National Association of Community Health Centers (NACHC).
The materials are offered 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.

This project is supported by the Health Resources and Services Administration (HRSA) of the U.S. Department of Health and Human Services (HHS) as part of an award totaling $6,375,000 with 0 percentage financed with non-governmental sources. The contents are those of the author(s) and do not necessarily represent the official views of, nor an endorsement, by HRSA, HHS, or the U.S. Government. For more information, please visit HRSA.gov

Main Office
7501 Wisconsin Ave
Suite 1100W
Bethesda, MD 20814
301.347.0400 TEL
301.347.0459 FAX
www.nachc.com

Federal and State Affairs
211 N. Union Street
Suite 200
Alexandria, VA 22314
703.739.7300 TEL
703.684.3629 FAX

Fact Sheet: Key Compliance Requirements Related to HIPAA and Telehealth

As increasing numbers of health centers embrace the use of telehealth, they must comply with a complex and complicated set of federal and state laws and regulations, including those related to payment, licensure and confidentiality. This Fact Sheet provides an overview of the key compliance requirements related to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and telehealth, suggesting steps health centers can take to protect patient information given that the risks have increased along with the heightened reliance on telehealth.

Introduction to the HIPAA Rules

The Office for Civil Rights (OCR) at the Department of Health and Human Services (HHS) enforces the "HIPAA Rules" which include:

- The Privacy Rule[1]: Addresses how individually identifiable health information, known as protected health information (PHI), can be used and disclosed with or without a patient's consent or authorization. The Privacy Rule also establishes standards for patients' privacy rights.
- The Security Rule[2]: Establishes standards to protect PHI that is created, received, used, or maintained in electronic form, known as electronic PHI (ePHI). The Security Rule requires covered entities and business associates to implement administrative, physical and technical safeguards in order to ensure the confidentiality, integrity, and security of ePHI.
- The Breach Notification Rule[3]: Requires covered entities and their business associates to provide notification following a breach of unsecured PHI.
- The Enforcement Rule[4]: Contains the provisions relating to compliance and investigations, the imposition of civil money penalties for violations of the HIPAA Rules, and procedures for hearings.

Together, the HIPAA Rules create a "floor" for protecting patient information and the compliance requirements for covered entities, such as health centers. Other federal and state laws and regulations provide additional protections for patient information and additional compliance requirements for health centers.

Telehealth Methods

While many people think of telehealth as the live video interaction between a health care provider and patient, telehealth services can also include store-and-forward, remote patient monitoring and mobile health. As described by the Center for Connected Health Policy[5], telehealth methods include:

- Live video (synchronous): Live, two-way interaction between a provider and another person (patient, caregiver or provider) using audiovisual telecommunications technology.
- Store-and-forward (asynchronous): Electronic transmission of videos and digital images through secure email communication.
- Remote patient monitoring (RMH): Use of digital technologies to collect medical and other forms of health data from individuals in one location and electronically transmit that information securely to health care providers in a different location for assessment and recommendations.

[1] 45 CFR Part 160 and Subparts A and E of Part 164.
[2] 45 CFR Part 160 and Subparts A and C of Part 164.
[3] 45 CFR §§ 164.400 – 414.
[4] 45 CFR Part 160, Subparts C, D, and E.
[5] https://www.cchpca.org/about/about-telehealth.

- Mobile health (mHealth): The provision of health care services and personal health data via mobile devices, such as cell phones, tablet computers, and personal devices.

The HIPAA Rules and Telehealth

The HIPAA Rules do not contain specific provisions related to telehealth. Instead, the HIPAA Rules are designed to be flexible and comprehensive to cover a variety of uses and disclosures of patient information. Below are examples of how the HIPAA Rules apply in the telehealth context. Each example contains compliance tips to help health centers develop HIPAA compliant telehealth services.

- **Content and Provision of the Notice of Privacy Practices[6]:** The HIPAA Privacy Rule requires a covered entity to notify patients as to how the covered entity will use and disclose the patient's PHI, the patient's rights, and the covered entity's legal duties with respect to PHI. The Notice of Privacy Practices must, among other things, describe and provide examples of the uses and disclosures of PHI that the covered entity is permitted to make without the patient's consent for purposes of treatment, payment and health care operations, along with a description of the other purposes for which the covered entity is permitted or required to use or disclose PHI without the patient's consent or authorization.

  Covered entities must provide the Notice of Privacy Practices on or before the patient's first appointment. If a patient's first visit is provided via telehealth, the covered entity must send the Notice of Privacy Practices electronically, automatically, and contemporaneously with the patient's first request for care (i.e. when the patient calls for an appointment). Covered entities must make a good faith effort to obtain written acknowledgement that the patient received the Notice of Privacy Practices. When the Notice of Privacy Practices is provided electronically, OCR has stated that "an electronic return receipt or other return transmission from the patient is considered a valid written acknowledgement of the notice."[7]

  Compliance Tips:
  - Revise the Notice of Privacy Practices to provide patients with information about the use of telehealth in your health center.
  - Ensure the updated Notice of Privacy Practices is posted on your health center's website and at each site; ensure that copies are available to those who request a copy.
  - Revise your health center's procedure for providing the Notice of Privacy Practices and obtaining patient acknowledgement to include a process for new patients receiving care via telehealth.

- **Security Management Process[8]:** Under the Administrative Safeguards section of the HIPAA Security Rule, the first standard requires covered entities and business associates to implement a security management process that includes four specifications: risk analysis, risk management, sanction policy and information system activity review.[9] The first two specifications are especially relevant in the context of telehealth. First, covered entities and business associates are required to "conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate." Next, they must "implement

[6] For more information on the Notice of Privacy Practices, *see* 45 CFR § 164.520.
[7] OCR, HIPAA for Professionals, FAQ 336, available at: https://www.hhs.gov/hipaa/for-professionals/faq/336/how-should-health-care-providers-provide-notice-when-treatment-is-over-the-phone/index.html.
[8] For more information on the Security Management Process, *see* 45 CFR §164.308(a)(1).
[9] *See* 45 CFR §164.308(a)(1).

security measures to reduce risks and vulnerabilities to a reasonable and appropriate level." Covered entities are expected to periodically perform a security risk analysis and conduct risk management activities. OCR has also stated that "a truly integrated risk analysis and management process is performed as new technologies and business operations are planned."[10]

Compliance Tips:

- Conduct an initial security risk analysis prior to implementing telehealth in your health center; update the security risk analysis periodically and prior to adding new telehealth technologies.
- Develop strategies to mitigate identified risks and vulnerabilities.
- Document your health center's efforts to mitigate the identified risks and vulnerabilities through a compliance work plan.

The security risk analysis and management activities often require review and revision of the Administrative, Physical and Technical Safeguards previously implemented by the covered entity. For example:

- Telehealth system access and controls may need review and revision to reflect:
  - How the telehealth platform connects to other systems (EMR, billing, etc.)
  - The audit controls necessary to record and examine activity in systems containing PHI

- Workforce security, management and training may need review and revision to reflect:
  - Employee access to the telehealth platform, including how access is granted, reviewed, revised and terminated
  - Locations from which employees are permitted to provide telehealth
  - Devices employees are permitted to use to provide telehealth services, including policies and procedures on the storage of PHI and on updating, reusing, and disposing of devices
  - Training for employees related to the telehealth platform, reporting security incidents and privacy and security for telehealth visits

- Incident procedures and plans may need review and revision to reflect:
  - Reporting of telehealth-related incidents through the current security incident procedures
  - Back up and restoration of data in the telehealth platform

- **Business Associates[11]:** Each of the HIPAA Rules includes requirements related to business associates. A business associate is a person or entity that performs certain functions, activities or services on behalf of a covered entity and the function, activity or service involves the use or disclosure of PHI. A business associate includes a person or entity that "creates, receives, maintains or transmits" PHI on behalf of a covered entity. OCR's 2013 Final Omnibus Rule modified the definition of a business associate to explicitly include "a Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information."[12]

---

[10] HIPAA Security Series #6 Basics of Risk Analysis and Risk Management, (page 16), available at: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf?language=es

[11] For more information on business associates, *see* 45 CFR §§ 164.502(e), 164.504(e), 164.532(d) and (e).

[12] 45 CFR § 160.103. In the 2013 Final Rule, OCR clarified that this definition includes a narrow exception for entities that are mere conduits of PHI, such as the U.S. Postal Service or internet service providers, and which do not have "access on a routine basis." A conduit "transports information but does not access it other than on a random or

Because telehealth vendors receive, maintain and transmit ePHI on behalf of covered entities, the HIPAA Rules require covered entities to have a written business associate agreement (BAA) or other arrangement in place with the telehealth vendor. The required elements of a BAA, outlined in the HIPAA Privacy Rule, include describing the permitted and required uses of PHI by the business associate, as well as the obligations and activities of the business associate. [13] If a covered entity knows that a business associate has committed a material breach or violation of the BAA, the covered entity is required to take reasonable steps or measures to cure the breach or end the violation. If those steps are unsuccessful, the covered entity must terminate the BAA. If terminating the BAA is not feasible, the covered entity is required to report to OCR.

Compliance Tips:

- Determine whether the telehealth vendor will sign your health center's BAA. If the telehealth vendor refuses and requires the use of their standard BAA, ask whether the vendor accepts edits to its standard BAA. If yes, your health center can attempt to include favorable terms. If not, ensure the BAA includes the required provisions and determine whether the terms, while not ideal, are acceptable to your health center.
- Track your health center's telehealth vendor contracts and business associate agreements to ensure they do not expire and to ensure they are readily available if/when there is an issue.

- **Breach Notification[14]:** Business associates are required to notify the covered entity upon discovery of a breach that occurs at or by the business associate. The business associate should identify the patients affected by the breach and include other information for the patient notice, such as a description of the breach, date of the breach and the date of discovery, and a description of the types of unsecured PHI involved. A covered entity can delegate responsibility for notifying the affected patients to the business associate.

  Compliance Tips:

  - Ensure the BAA with your health center's telehealth vendor details the reporting of potential breaches, including a timeframe for such reports and identification of the appropriate health center contact (CEO, Compliance Officer, Security Officer, etc.).
  - Include a provision providing the health center with flexibility to delegate its notification requirements to the business associate.

Conclusion

Every health center must weigh the benefits of telehealth – increased patient and provider satisfaction, expanded access to specialists, and increased safety for patients, providers, and other health center employees – against the compliance risks. As detailed in this Fact Sheet, the HIPAA Rules provide a framework for health centers to identify, analyze and respond to the privacy and security risks in the telehealth setting.

---

infrequent basis as necessary to perform the transportation service or as required by other law" (78 Fed. Reg. 5571). Telehealth vendors, which regularly receive, access, and transmit PHI, as well as maintain PHI, on behalf of covered entities, generally do not fit the conduit exception and therefore are business associates. Health center should consult with legal counsel prior to contracting with a telehealth vendor unwilling to sign a business associate agreement (BAA).

[13] The BAA must contain all the elements at 45 CFR § 164.504(e).

[14] For more information on breach notification by a business associate, *see* 45 CFR § 164.410.

Fact Sheet: HIPAA Compliance Flexibilities Related to Telehealth During COVID-19

As health care providers worked to develop new care models during the early months of the COVID-19 pandemic public health emergency, the Office for Civil Rights (OCR) at the Department of Health and Human Services (HHS) announced important flexibilities related to telehealth services. OCR, which is responsible for enforcing the Privacy, Security and Breach Notification Rules issued under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (the HIPAA Rules), recognized that telehealth could allow health care providers to assess a greater number of patients for COVID-19 while limiting the risk of spreading COVID-19 to other patients and staff members. OCR also realized that many health care providers, unprepared for the move to telehealth, would rely on everyday communication products. Those products and the ways in which they were likely to be used were unlikely to fully comply with the HIPAA Rules. This would put health care providers in the untenable position of choosing between providing telehealth visits using technology that was not HIPAA-compliant or leaving patients without care while implementing a HIPAA-telehealth program.

On March 17, 2020, OCR issued a Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency (Notification of Enforcement Discretion). OCR summarized the effect of the Notification of Enforcement Discretion by stating that:

> *OCR is exercising its enforcement discretion to not impose penalties for noncompliance with the HIPAA Rules in connection with the good faith provision of telehealth using such non-public facing audio or video communication products during the COVID-19 nationwide public health emergency.*

The Notification of Enforcement Discretion provided immediate flexibility for certain covered entities using telehealth communication products that meet OCR's criteria. Below, we examine the Notification of Enforcement Discretion in detail, incorporating additional guidance from the FAQs on Telehealth and HIPAA during the COVID-19 nationwide public health emergency (FAQs on Telehealth) issued separately by OCR. Health centers should use this period of flexibility strategically to assess the available telehealth communication products and to engage with a HIPAA-compliant telehealth vendor before the Notification of Enforcement Discretion is rescinded.

Flexibility under OCR's Notification of Enforcement Discretion

To understand the flexibilities under the Notice of Enforcement Discretion and the limits on those flexibilities, OCR's summary statement above is examined in more detail here.

> **OCR will exercise its enforcement discretion and will not impose penalties for noncompliance with the regulatory requirements under the HIPAA Rules**

The Director of OCR is authorized to impose civil monetary penalties (CMPs) against any HIPAA covered entity that violates the HIPAA Rules. Under the Health Information Technology for Economic and Clinical Health (HITECH) Act, OCR is authorized to impose CMPs ranging from $100 per violation to $50,000 per violation with annual limits ranging from $25,000 to $1.5 million per year, depending upon the covered entity's culpability.[1]

[1] These amounts are updated for inflation each calendar year. The penalty amounts for 2020 are available at 85 Fed. Reg. 2869.

Under the Notification of Enforcement Discretion, OCR stated that it will not impose penalties for noncompliance with the HIPAA Rules related to a health care provider's good faith provision of telehealth services during the COVID-19 nationwide public health emergency, including when a covered provider fails to execute a business associate agreement (BAA) with a vendor providing telehealth services, including those vendors providing everyday communication products. The HIPAA Rules define a business associate as a person or entity that performs certain functions, activities or services on behalf of a covered entity and that creates, receives, maintains or transmits protected health information in providing the functions, activities, or services. In this context, a telehealth vendor is a business associate because it provides data transmission services and it requires access on a routine basis to protected health information in order to provide the data transmission services.[2]

While health care providers may execute a BAA with their telehealth vendor, they will not face penalties from OCR for not executing such a BAA during the COVID-19 nationwide public health emergency. As discussed below, in the Notification of Enforcement Discretion, OCR encourages health care providers to engage with telehealth vendors that will sign a BAA and, once the Notification of Enforcement Discretion is rescinded, a BAA will be required.

Covered health care providers

The Notification of Enforcement Discretion applies only to health care providers; it does not apply to other HIPAA covered entities, such as health insurance plans. Because health centers provide health care services which are billed electronically, they are considered covered health care providers.

Telehealth services

Telehealth, defined by the Health Resources and Services Administration (HRSA) as the "use of electronic information and telecommunications technologies to support and promote long-distance clinical health care, patient and professional health-related education, and public health and health administration," includes landline and wireless communications, videoconferencing, store-and-forward imaging, streaming media, and internet technologies. Telehealth services may be provided through videoconferencing software, audio, text messaging or other video communication technology.

OCR makes clear that all services that a covered health care provider believes, in their professional judgement, can be provided through telehealth and are covered by the Notification of Enforcement Discretion. As explained in the FAQ on Telehealth, this includes the "diagnosis or treatment of COVID-19 related conditions, such as taking a patient's temperature or other vitals remotely, and diagnosis or treatment of non-COVID-19 related conditions, such as review of physical therapy practices, mental health counseling, or adjustment of prescriptions, among many others."

Provided in good faith

OCR states that it would consider all facts and circumstances when determining what constitutes a good faith provision of telehealth services. OCR provides the following example of good faith provision of telehealth services: if a provider follows the terms of the Notification of Enforcement Discretion and any applicable OCR guidance (including the FAQ on Telehealth), the health care provider would not face HIPAA penalties if it experiences a hack that exposes protected health information from a telehealth session.

OCR provides several examples of the bad faith provision of telehealth services:

[2] *See* 45 CFR § 160.103.

- Conduct or furtherance of a criminal act, such as fraud, identity theft, and intentional invasion of privacy;
- Further uses or disclosures of patient data transmitted during a telehealth communication that are prohibited by the HIPAA Privacy Rule (*e.g.*, sale of the data, or use of the data for marketing without authorization);
- Violations of state licensing laws or professional ethical standards that result in disciplinary actions related to the treatment offered or provided via telehealth (*i.e.*, based on documented findings of a health care licensing or professional ethics board); or
- Use of public-facing remote communication products.

In each of these examples, the Notification of Enforcement Discretion would not apply and the health care provider would face HIPAA penalties.

Non-public facing audio or video communication products

As described above, the Notification of Enforcement Discretion only applies when the covered health care provider uses non-public facing audio or video communication products. These technologies allow only the intended individuals to participate in the communication. These products typically use end-to-end encryption which allows only the sender and intended recipient to see what is transmitted. These products use individual user accounts, passcodes, logins and user controls to limit unintended access, verify participants and provide control over recording, video and sound functions. OCR identified several popular applications that allow for non-public facing communication, including:

Non-Public Video Applications	Non-Public Texting Applications
Apple FaceTime	Signal
Facebook Messenger video chat	Jabber
Google Handouts video	Facebook Messenger
Skype	Google Hangouts
Whatsapp video chat	iMessage
Zoom	Whatsapp

Public facing remote communication products are not covered by the Notification of Enforcement Discretion and therefore should not be used to provide telehealth services. Such products are designed to be open to the public or allow wide access to the communication. Public-facing remote communication products include Facebook Live, TikTok, Twitch, and public chat rooms.

During the COVID-19 nationwide public health emergency:

The Notification of Enforcement Discretion went into effect immediately and does not have an expiration date. OCR stated that it will issue a notice to the public when it is no longer exercising its enforcement discretion. OCR has not indicated whether there will be a period for health care providers to comply with the HIPAA Rules after the Notice of Enforcement Discretion is rescinded.

OCR's Other Expectations

Throughout the Notification of Enforcement Discretion Notice and the Telehealth FAQ, OCR reminds health care providers about their other compliance requirements and provides recommendations for

protecting the privacy and security of protected health information. OCR expects health care providers will:

- Enable all available encryption and privacy modes when using non-public facing remote communication applications;
- Notify patients that non-public facing remote communication applications potentially introduce privacy risks;
- Conduct telehealth sessions from a private setting, such as a clinic or office space, and, if that is not possible, implement reasonable HIPAA safeguards such as using a lowered voice or avoiding use of a speakerphone;
- Encourage patients to attend telehealth session from a private setting and, if that is not possible, recommend the patient move a reasonable distance from others;
- Engage with telehealth vendors that will protect protected health information by signing a BAA; and
- Maintain compliance with the applicable HIPAA Rules in all areas outside of telehealth.

Checklist[1]: Key HIPAA-Related Questions for Telehealth Vendors[2]

1. Does the telehealth platform protect patient information during transmission with strong encryption?

2. What patient information is maintained in the telehealth platform – patient name, contact information, appointment date, provider information, appointment type, payment information, chat logs, recordings of the telehealth visit, etc.? How does the telehealth platform protect patient information it maintains? How long is patient information maintained? How is patient information returned or destroyed?

3. Does the telehealth platform consolidate/match patient information from various covered entities? Does the telehealth platform provide any other health information exchange capacities?

4. Does the telehealth platform store visit information on the system or device used for the visit (*i.e.*, employee or patient devices)? What is the default setting for such storage? How can it be altered?

5. How does the telehealth vendor monitor access to the telehealth platform by its employees, health center employees and patients? How often is there an internal audit to ensure health center's employees have appropriate access (i.e. a terminated employee does not still have access)?

6. How many licenses to the telehealth platform are included in the contract for health center staff? Who is responsible for assigning, monitoring and terminating licenses?

7. How frequently does the system require password to be updated? How is the identity of staff members verified? How frequently is their identity verified?

8. What training is required and/or recommended for health center staff who use the telehealth platform? Does the telehealth vendor provide training or training materials?

9. How do patients access the telehealth platform? How is their identity verified? How frequently is their identity verified?

10. What information is available to patients in the telehealth platform? If their log-in information was compromised, what information would be visible (provider

[1] The Authors of these materials include attorneys at the law firm of Feldesman Tucker Leifer Fidell LLP. This document provides general guidance based on certain federal laws and regulations. The information does not necessarily apply to all health centers under all facts and circumstances. Further, these materials do not replace, and are not a substitute for, legal advice from qualified legal counsel.

[2] The questions set forth herein reflect obligations under and relating to the Health Insurance Portability and Accountability Act of 1996, Pub L. 104-191, ("HIPAA") and the regulations promulgated thereunder by the U.S. Department of Health of Health and Human Services, found at 45 CFR Parts 160 and 164 ("HIPAA Rules"). Other federal and state laws relating to the use or disclosure of patient information may apply and may be more restrictive than those of HIPAA and should be consulted.

information, appointment type, payment information, chat logs, recordings of telehealth visits)?

11. If the telehealth platform fails mid-appointment, what is the process for reporting and investigating the issue, as well as reconnecting the patient and provider?

12. Does the telehealth platform require and/or recommend integration with other health center systems, such as payment terminals, accounts receivable or other systems that contain financial information? What are the security risks associated with such integration? Is the telehealth vendor familiar with the systems used by the health center and whether they can be integrated?

13. Will the telehealth vendor provide support in installing any required software or applications? What system access will be required for installation?

14. How frequently is the telehealth platform updated? Who is responsible for such updates? Will such updates require the telehealth platform to be unavailable for a period of time?

15. Is the telehealth platform run from systems owned and maintained (hosted) by the vendor? Does the contract state that the telehealth vendor maintains such systems in compliance with all applicable laws, regulations and standards?

16. How frequently does the telehealth vendor conduct a security risk analysis?

17. What monitoring for data breaches and suspicious activities does the telehealth vendor provide? How and when will the health center be notified of a potential breach?

18. What support will the telehealth vendor provide if there is a breach (caused by the vendor)? What if the health center is fined?

19. Does the telehealth vendor have cybersecurity and data breach insurance? What is the scope of coverage and will the health center's use of the telehealth platform be covered?

Checklist[1]: Business Associate Agreements for Telehealth Vendors[2]

Introduction/Recitals:

- ☐ Identify the parties to the business associate agreement (BAA) are identified (health center as Covered Entity and telehealth vendor as Business Associate).
- ☐ Explain relationship of the parties by reference to underlying service agreements or include details of the activities, functions, or services to be performed by Business Associate which involves the use and disclosure of protected health information (PHI) or for which Business Associate will create, receive, maintain or transmit PHI on behalf of Covered Entity.

Obligations and Activities of Business Associate:

- ☐ Restrict the Business Associate's use or disclosure of PHI to uses or disclosures that are permitted or required by the BAA or required by law.

- ☐ Require Business Associate to use appropriate safeguards to prevent unauthorized use or disclosure of the information, including implementing requirements of the HIPAA Security Rule with respect to electronic PHI.

- ☐ Require Business Associate to report to the Covered Entity any use or disclosure of the information not provided for by its contract, including incidents that constitute breaches of unsecured PHI.
  - Optional: Requires Business Associate to report potential breaches to the Covered Entity within a shorter timeframe.
  - Optional: Include flexibility for Covered Entity to require Business Associate to notify individuals, the Office for Civil Rights (OCR), and the media (if applicable) of breaches.

- ☐ Require Business Associate to ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of Business Associate agree to the same restrictions, conditions and requirements that apply to the Business Associate with respect to the PHI.

- ☐ Require Business Associate to make available PHI in accordance with an individual's access rights under 45 CFR § 164.524.

- ☐ Require Business Associate to make any amendments to PHI in accordance with 45 CFR § 164.526.

---

[1] The Authors of these materials include attorneys at the law firm of Feldesman Tucker Leifer Fidell LLP. This document provides general guidance based on certain federal laws and regulations. The information does not necessarily apply to all health centers under all facts and circumstances. Further, these materials do not replace, and are not a substitute for, legal advice from qualified legal counsel.

[2] The terms set forth herein reflect obligations under and relating to the Health Insurance Portability and Accountability Act of 1996, Pub L. 104-191, ("HIPAA") and the regulations promulgated thereunder by the U.S. Department of Health of Health and Human Services, found at 45 CFR Parts 160 and 164 ("HIPAA Rules"). The requirements for business associate agreements can be found at 45 CFR § 164.504(e). Other federal and state laws relating to the use or disclosure of patient information may apply and may be more restrictive than those of HIPAA and should be consulted.

- Require Business Associate to maintain and make available the information required to provide an accounting of disclosures in accordance with 45 CFR § 164.528.

- To the extent the Business Associate is to carry out Covered Entity's obligation(s) under the Privacy Rule, require Business Associate to comply with the requirements that apply to the Covered Entity in the performance of such obligation.

- Require Business Associate to make its internal practices, books, and records relating to the use and disclosure of PHI received from or created or received by the Business Associate on behalf of the Covered Entity available to the Secretary of HHS for purposes of determining the Covered Entity's compliance with the Privacy Rule.

- Require that Business Associate may not threaten, intimidate, coerce, harass, discriminate against, or take any other retaliatory action against any person for, in relation to the BAA or underlying service agreement, filing a complaint with the Secretary for perceived HIPAA violations; testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing involving a perceived HIPAA violation; or opposing any act or practice made unlawful by HIPAA, provided the person has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not involve a prohibited disclosure of Covered Entity's PHI.

Uses and Disclosures by Business Associate

- Permit Business Associate to use or disclose PHI:
  - Option 1: As listed in BAA
  - Option 2: As necessary to perform the functions, activities and services set forth in an underlying service agreement

- Permit Business Associate to use or disclose PHI as required by law.

- Permit Business Associate to make uses, disclosures and requests for PHI:
  - Option 1: Consistent with Covered Entity's minimum necessary policies and procedures
  - Option 2: Subject to the following minimum necessary requirements: [*list specific minimum necessary provisions consistent with Covered Entity's minimum necessary policies and procedures*].

- Business Associate may not use or disclose PHI in a manner that would violate the HIPAA Privacy Rule if done by the Covered Entity, except for the uses and disclosures set forth below (if any):

  - Optional: May permit Business Associate to provide data aggregation services relating to the health care operations of Covered Entity.
  - Optional: May permit Business Associate to:
    - Use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

- Disclose PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate if:
  - The disclosure is required by law; or
  - Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

Term and Termination

☐ List the effective date and the termination date or event, including Covered Entity's ability to terminate for cause.

☐ Authorize termination of the contract by the Covered Entity, if the Covered Entity determines that the Business Associate has violated a material term of the contract.

☐ Require that at termination of the contract:
- Business Associate shall return or destroy all PHI received from, or created or received by the Business Associate on behalf of, the Covered Entity that the Business Associate still maintains in any form and retain no copies of such information.
- If return or destruction is not feasible, Business Associate shall extend the protections of the BAA to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.
- If BAA authorizes Business Associate to use or disclose PHI for its own management and administration or to carry out its legal responsibilities, Business Associate shall:
  - Retain only the PHI which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;
  - Return to Covered Entity or destroy the remaining PHI that Business Associate still maintains in any form;
  - Continue to use appropriate safeguards and comply with HIPAA Security Rule with respect to electronic PHI to prevent use or disclosure of the PHI for as long as Business Associate retains the PHI;
  - Not use or disclose the PHI retained by Business Associate other than for the purposes for which such PHI was retained and subject to the same conditions set out in the BAA which applied prior to termination; and
  - Return to Covered Entity or destroy the PHI retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.

Other Provisions

☐ Ensure survival of the following provisions:
- Requirement for Business Associate to make its internal practices, books, and records relating to the use and disclosure of PHI received from or created or received by the Business Associate on behalf of, the Covered Entity available to the Secretary

of HHS for purposes of determining the Covered Entity's compliance with the Privacy Rule.

- Any PHI retained under the Termination Provisions

Tool[1]: Telehealth Vendor and Business Associate Agreement (BAA) Tracker[2]

Vendor Name	Vendor Contact Information[3]	BAA Execution Date	BAA Expiration Date	BAA Template or Other[4]	Telehealth Services Provided[5]	Types of Patient Information[6]	Additional Agreement/ Consent Required[7]
Sample Telehealth Vendor	*Compliance Officer: 202-466-8960*	*3/15/20*	*3/15/21*	*Other: BA to report potential breach w/in 15 calendar days*	*Live video*	*Medical, behavioral health, HIV status*	*Patient consent for HIV status (per state law)*

[1] The Authors of these materials include attorneys at the law firm of Feldesman Tucker Leifer Fidell LLP. This tool provides general guidance based on certain federal laws and regulations and does not necessarily apply to all health centers under all facts and circumstances. Further, these materials do not replace, and are not a substitute for, legal advice from qualified legal counsel.

[2] The items set forth herein reflect obligations under and relating to the Health Insurance Portability and Accountability Act of 1996, Pub L. 104-191, ("HIPAA") and the regulations promulgated thereunder by the U.S. Department of Health of Health and Human Services, found at 45 CFR Parts 160 and 164. Other federal and state laws relating to the use or disclosure of patient information may apply and may be more restrictive than those of HIPAA and should be consulted.

[3] Consider including contact information for the vendor's CEO, Compliance Officer and Security Officer.

[4] Document whether the health center's BAA template was executed with. If the health center's template was amended, note any relevant amendments here (for example, if the business associate has a longer time period to report potential breaches). This information can serve as a quick reference for the health center if/when there is an issue with the business associate.

[5] Include details as to the telehealth method provided by the vendor: live video (synchronous), store-and-forward (asynchronous), remote patient monitoring (RMH), and/or mobile health (mHealth).

[6] Include the types of patient information to be disclosed to the vendor or created, received, maintained or transmitted by the vendor on behalf of a covered entity. If information protected by other federal and state laws is disclosed, ensure either the Underlying Services Agreement, the BAA or other agreements address the compliance requirements related to the disclosure of such patient information.

[7] Include additional agreements and/or consent requirements under federal and state laws and regulations.