Ethics, Security, and Confidentiality

by Capella Healthcare

WHAT'S COVERED

In this lesson, you will learn about the ethics, security, and confidentiality related to telehealth. Specifically, this lesson will cover:

1. Privacy and Security
2. Informed Consent
3. How to Obtain Consent for Telehealth
4. Reflect: HIPAA and Your Telehealth Patient

1. Privacy and Security

HIPAA (Health Insurance Portability and Accountability Act), **COPPA** (Children's Online Privacy Protection Act), and **HITECH** (Health Information Technology for Economic and Clinical Health) Act requirements all apply to telehealth visits (Balestra, M., 2018). These requirements apply to both in-person visits as well as telehealth visits, but they extend to identifying specific requirements relating to telehealth technology; there is guidance within each which ensure the privacy and security of patients and secure health information (Bhate, C. et al., 2020).

It is important to consider a patient's personal information, whether it is **protected health information (PHI)** or **electronic protected health information (ePHI)**. The HIPAA guidelines on telemedicine require that only authorized users should have access to patient ePHI, secure communication must be used (not FaceTime or Skype or Facebook, etc.) to protect ePHI, and a method must be available to monitor the communications containing the ePHI for potential breaches of data (American Telemed Association, 2020). In addition, if you are creating ePHI in any form (medical records, images, data from an eHealth app, billing, transcription, legal, etc.) that is stored by a third party, you are required by HIPAA to also have a Business Associate Agreement (BAA) executed with the third party. The BAA must outline how the third party will ensure the protection of the ePHI/data as well as detailed provisions for regular auditing of the data's security. A **business associate** is any third party that performs functions or activities on behalf of a **covered entity** that requires them to have access to or store PHI or ePHI.

HINT

Specifics on IT requirements and cybersecurity are covered in another lesson of this course.

The government has provided a HIPAA audit protocol (HHS Secretary-Office of Civil Rights, 2018) that

provides details relating to the internal security and privacy protection requirements for healthcare systems. However, this protocol is complicated and includes extensive details that are not always specific to telehealth. Therefore, interpreting the protocol details is challenging. Zhou et al. (2019) have developed and validated a telehealth privacy and security self-assessment questionnaire for telehealth providers. This is one example of a validated instrument that provides a statistically reliable means for telehealth providers and professionals to self-assess their telehealth systems and programs for HIPAA compliance based on the current security and privacy rules in telehealth practices.

Patient confidentiality and privacy are high on the list of both patient and provider concerns. Protected health information breaches are costly mistakes. As reported in the Cost of Data Breach Report 2020 released by IBM Security and the Ponemon Institute, the average global cost of a health data breach was 3.87 million U.S. dollars, with healthcare being the most “at-risk” and “costly” industry (Ponemon Institute & IBM Security, 2020).

TERMS TO KNOW

HIPAA
Health Insurance Portability and Accountability Act of 1996; provides guidance on protecting sensitive patient health information.

COPPA
Children’s Online Privacy Protection Act of 1998; provides guidance on protecting what information is collected from young children online.

HITECH
Health Information Technology for Economic and Clinical Health of 2009; provides guidance on the use of health information technology.

Protected Health Information (PHI)
Any personal information within a medical record that may be used to identify an individual.

Electronic Protected Health Information (ePHI)
Any electronic personal information within a medical record that may be used to identify an individual.

Business Associate
Any third party that performs functions or activities on behalf of a covered entity that requires them to have access to or store PHI or ePHI.

Covered Entity
Anyone who provides treatment, payment, and operations in healthcare.

2. Informed Consent

Many states and payers require you to obtain patient consent, or **informed consent**, in order for you to be reimbursed for patient care. The purpose of informed consent is to document that a discussion took place and the patient was informed of and able to understand the information provided. Some states require written consent, some verbal, and some none. Also, some states have specific Medicaid requirements regarding consent. It is important to understand the regulations in the state where you practice as well as the state where the patient resides (if the two are different).

Even if informed consent is not specifically required in your state, it is best practice. The American Telemedicine Association (2020) suggests the informed consent form should include the following:

- "Inform patients of their rights when receiving telemedicine, including the right to stop or refuse treatment;
- Tell patients their own responsibilities when receiving telemedicine treatment;
- Have a formal complaint or grievance process to resolve any potential ethical concerns or issues that might come up as a result of telemedicine;
- Describe the potential benefits, constraints, and risks (like privacy and security) of telemedicine;
- Inform patients of what will happen in the case of technology or equipment failures during telemedicine sessions, and state a contingency plan."

Additionally, The American Society for Healthcare Risk Management recommends:

- State specific requirements
- The names and credentials of telemedicine staff and providers
- Technology that will be used
- Permission to bill as applicable
- Instructions for alternative care in case of emergency or technology malfunction

Best practice is to also outline any telemedicine policies regarding scheduling, access requirements, scheduling, cancellation (including fees), etc. (American Academy of Allergy, Asthma & Immunology, 2020).

TERM TO KNOW

Informed Consent
The process in healthcare where a patient voluntarily provides permission to undergo care following a full explanation on the risks, benefits, and alternatives.

3. How to Obtain Consent for Telehealth

Before the consent discussion:

- Use your patient portal or the mail to send your patient the form in advance of the visit, so they have adequate time to read it. There should also be a video or audio of the informed consent to meet literacy levels and those with vision impairment. When possible, create versions with the languages of the three largest ethnic populations in your service area.
- Arrange for a qualified interpreter if your patient is not English speaking. The interpreter should be part of the entire consent discussion.

During the consent discussion:

- Use the consent form as a checklist to ensure you cover all of the topics required from informed consent rules.
- Use easy-to-understand language following **health literacy guidelines** from the Center for Disease Control.
- Use the **teach-back method** to verify patient understanding.
- Document teach-back with the **Telehealth Consent Teach-back documentation sheet**

- Start with a phrase like, “It’s my job to explain clearly. To make sure I’m doing a good job, I usually ask every patient to tell me what you understand about telehealth and how it might help you.”
- "Chunk and Check." Don’t wait until the end to teach-back. Parcel out information into small chunks and have your patient teach it back. For example, ask patients “Could you tell me in your own words what will happen to you if you decide you want a telehealth visit?”
- Clarify and check again if there is a misunderstanding. Explain things again using a different approach. Ask patients to teach-back again until they are able to correctly depict the information in their own words. If they give you a verbatim or read the form back to you, they may not have understood.

Before asking patients if they agree to the telehealth visit:

- Ask patients if they have any questions. You could say, “Since we covered so much information, I’m sure you may some questions. Is there anything you would like to hear more about?”
- Ask open-ended questions so as not to elicit a yes or no answer.

After the consent discussion:

- Document patient’s ability to teach the information back correctly in the medical record.
- If patients decline to consent, note it in their medical record.
- If patients consent, obtain patient’s consent verbally and note it in the medical record. If you need a signed form, use your patient portal or mail to get a signature. DocuSign or other electronic signature platforms may also be an option.
- Ask patients if they are able to access the portal. If not, direct them to staff who can assist.
- If you mail the consent forms, send an extra copy for the patient to keep and send a pre-paid postage return envelope for them to mail it back. Once the form is returned, enter it into the medical record.
- You do not need to wait to get the consent signed. You can have telehealth visits based on the patient giving verbal consent.

4. Reflect: HIPAA and Your Telehealth Patient

Review this **example** of an Informed Consent for telehealth and consider the following points:

Per federal regulations, the following are the required elements for documentation of the informed consent discussion:

1. *The nature of the procedure or intervention (in this case, telehealth)*
2. *The risks and benefits and the procedure or intervention*
3. *Reasonable alternatives (if applicable)*
4. *Risks and benefits of those alternatives*
5. *Assessment of the patient’s understanding of elements 1 through 4*

REFLECT

1. Do you feel the informed consent form example addresses each of these aspects? Why or why not?
2. Is there anything else you think should be included?

Authored by Cindy Ebner, MSN, RN, CPHRM, FASHRM and Melissa A. Singer Pressman, PhD, MLIS

Support

If you are struggling with a concept or terminology in the course, you may contact **TelehealthSupport@capella.edu** for assistance.

If you are having technical issues, please contact **learningcoach@sophia.org**.

TERMS TO KNOW

Business Associate
Any third party that performs functions or activities on behalf of a covered entity that requires them to have access to or store PHI or ePHI.

COPPA
Children's Online Privacy Protection Act of 1998; provides guidance on protecting what information is collected from young children online.

Covered Entity
Anyone who provides treatment, payment, and operations in healthcare.

Electronic Protected Health Information (ePHI)
Any electronic personal information within a medical record that may be used to identify an individual.

HIPAA
Health Insurance Portability and Accountability Act of 1996; provides guidance on protecting sensitive patient health information.

HITECH
Health Information Technology for Economic and Clinical Health of 2009; provides guidance on the use of health information technology.

Informed Consent
The process in healthcare where a patient voluntarily provides permission to undergo care following a full explanation on the risks, benefits, and alternatives.

Protected Health Information (PHI)
Any personal information within a medical record that may be used to identify an individual.