Compliance Today - December 2020
Is your telehealth environment ready for 2021?

By Carol L. Amick, CHC, CHPC, CPA

Carol L. Amick (camick@compliancepoint.com) is Director of Healthcare Services at CompliancePoint in Duluth, GA.

As all of us can attest, 2020 has been a unique year, one that we are unlikely to ever forget! When you think about that time-honored interview question, "Where do you see yourself in five years?" I don't think anyone can say they expected to be dealing with a pandemic that could have significant changes in the delivery model for healthcare for the future.

COVID-19 has dramatically changed the way healthcare is delivered. Providers were forced to pivot quickly from total reliance on in-person visits to almost total reliance on alternative delivery methods. A recent McKinsey & Company survey stated that telehealth adoption soared "from 11 percent of US consumers using telehealth in 2019 to 46 percent of consumers now using telehealth."[1] McKinsey & Company predicted that up to $250 billion of the current healthcare spending could transition to telehealth and that consumers were significantly more likely to use telehealth going forward. Providers also view telehealth more favorably than they did before COVID-19. A recent Accenture survey also supported increased adoption of telehealth, noting that 60% of patients surveyed want to continue to use telehealth services in the future.[2]

One of the facilitating factors for the rapid move to telehealth was the decision by the Office for Civil Rights (OCR) at the Department of Health & Human Services to exercise its enforcement discretion related to potential Health Insurance Portability and Accountability Act (HIPAA) violations in connection with good-faith use of telehealth services.[3] The OCR guidance indicated that providers could use popular applications such as FaceTime, Google Hangouts, or Zoom to provide telehealth.[4] The OCR did caution against using any public-facing application such as Facebook Live or TikTok. The OCR waiver, combined with changes in reimbursement models, has allowed telehealth to become a much more relevant care delivery method.

While there are several compliance concerns related to consent, care delivery, and billing that a compliance officer needs to consider when evaluating their organization's compliance with telehealth, you cannot afford to ignore privacy and security risks related to telehealth. Performing an assessment of your telehealth environment now, while the OCR is granting us this grace period, will help reduce the future risk to your organization. Additionally, while the OCR may not be exercising its enforcement efforts, a breach of protected health information (PHI) related to telehealth could still have devastating impacts on your organization and the organization's reputation in your community.

Securing your telehealth environment

Consumers are still concerned about the privacy of their PHI in the telehealth world. One recent survey indicated that more than 25% of consumers surveyed were worried about the privacy of their PHI.[5] This concern is only heightened by media reports outlining the risk of video call hijacking or zoom bombing. As students return to school via virtual platforms, the concerns over security will only be heightened. One school system in North

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

Carolina reported more than a dozen instances of zoom bombing in the first four days of the school year in August 2020.[6] In order to increase consumer acceptance and ensure continued compliance with HIPAA requirements, organizations that have implemented telehealth in response to the COVID-19 pandemic need to take steps to secure their telehealth environment.

Step one: Identify your deliverymethods

How many telehealth services are you using to provide care? If you did not have an in-place model in early March, there's a considerable risk that your providers have found services to use possibly without going through your normal vendor assessment process. Recently, one provider with an extensive provider network was quoted as indicating her organization had providers using FaceTime, Zoom, Cerner, and other telecommunication platforms.[7] Before you can secure your environment, you need to get a good understanding of what your providers are using. You will then need to make some decisions.

Do you continue to allow providers to pick their solution, or do you go with a standardized product throughout the organization? Of course, if you find that your providers are using Facebook Live, the decision is easy—that tool must go. But it becomes more complicated if you have providers using a multitude of other vendors.

While allowing your providers to use their favorite delivery method might make you popular with the providers, it is also going to increase the amount of time and work required to secure your environment. Additionally, your organization may also want to consider the impact of having different telehealth delivery platforms from different providers on the patients.

Step two: Evaluate your vendors

Once you have inventoried your providers, you need to do a vendor evaluation. This should be done regardless of how many vendors you have. This vendor evaluation can also help you reduce the number of products being used. This evaluation will need to be performed with a cross-functional team. While compliance will want a product that protects PHI, the product also needs to be user friendly to both your providers and your patients. Working as a team will help you identify products that satisfy all your needs.

Performing a vendor security assessment will demonstrate your efforts to ensure your vendor is complying with the HIPAA regulations. Remember that even if the telehealth vendor has the breach, your organization will be subject to both potential reputational damage and a review by OCR to verify you had appropriate controls in place. At a minimum, your vendor assessment should include the following:

- Is the vendor HIPAA compliant? Can they provide you with independent evidence of that compliance?
- If the vendor has a healthcare-specific software, are you using the correct version?
- Does the vendor have any security certifications, such as HITRUST?
- Have they provided you details on what they do with your data? Are they maintained by the vendor? If so, how are they stored and what protections are in place?
- Do they have policies and procedures in place for privacy and security?
- Have they done a risk assessment and addressed identified risks?
- What is their communication protocol? Do they have protections to stop zoombombing?

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

- Do they train their personnel on the protection of PHI?
- Do they have a well-developed incident response plan?

After you complete your assessment and are satisfied with the vendor's privacy and security practices, do not forget to execute a business associate agreement (BAA) outlining their responsibilities. Some telehealth vendors are reluctant to sign BAAs because they claim they are only conduits and do not hold or have access to the information. If you are relying upon that exception, be sure your understanding of the data flow agrees with that of the vendor. If OCR believes you should have had a BAA and you have a data breach, you run the risk of potentially increased regulatory attention and costs. A recent OCR settlement of more than $1 million specifically called out the failure to have a BAA in place.[8]

Step three: Secure your environment

Now that you know whom you are going to use and are reasonably certain that they are protecting your data, you need to look at your environment.

The Cybersecurity and Infrastructure Security Agency has developed "Guidance for Securing Video Conferencing."[9] While not specific to healthcare, it does give you a road map for establishing a secure environment. The guidance can assist you in securing your telehealth service environment. The Cybersecurity and Infrastructure Security Agency has identified four principles that you should consider for securing video conferencing:

1. **Connect securely.** Make sure the settings on Wi-Fi networks and your delivery tools are secure. Change the default passwords and make sure your wireless network has at least a WPA2 encryption. If your providers are delivering care from their home, you need to make sure their wireless networks are also secured. Default passwords and weak encryption make it incredibly easy for hackers to gain access to your PHI. Remember the Equifax data breach of 147 million consumers in 2017? Some experts believe that breach could have been prevented by the removal of default passwords.[10]

2. **Control access.** Enable the security and privacy setting on your telehealth tool. Ensure that your tool requires the provider to manually accept attendees to the conference by the use of "waiting rooms." Consider the need to require access codes or passwords for access to the visit.

3. **Manage screen sharing and recordings.** When doing a screen share during a telehealth visit, ensure that you are sharing only the correct information. Best practices would require that the provider close all screens, reports, etc., that would have data not related to the patient showing. You do not want the provider to accidentally show their daily patient list or the wrong lab results to a patient. Verify recordings of the telehealth visits are stored securely using encryption. If providers record the visits, make sure they are aware of the restrictions on the use of the recordings to prevent them being from stored in an unsecured manner.

4. **Keep your tool updated**. Telehealth service providers should be updating their tools to address newly identified security risks. Zoom, for example, had more than 30 updates between April and June 2020.[11] However, if your tool does not have the most recent software, you may not be adequately protected. Management of the telehealth tool should be handled just like the management of any other information technology asset at your facility.

Securing your environment also extends to securing the devices used for telehealth. One recent report indicated

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

that more than a third of all workstations in healthcare operate on unsupported versions of Windows, which exposes them to significant security risks.[12] All devices—both organization-owned and personal devices—should be managed using a mobile device management tool that is password protected, encrypted, and has up-to-date anti-malware software and other security measures. Remember that million-dollar settlement discussed above? In addition to the failure to have a BAA, they also had unencrypted laptops![13]

Your network should be configured to approve both the user and the device before allowing access and automatically log off inactive sessions. Logging of network activity should be done, and logs should be audited to identify potentially unusual activity.

Step four: Train your providers and staff

Make sure your training is enhanced to address the risks of telehealth. Specifically, training should remind providers that telehealth should be delivered in a secure manner—they should be aware of where they are and who can overhear them. Delivering telehealth in a public space or in front of their family could result in a HIPAA violation. Remember, the current COVID-19 HIPAA enforcement waiver only protects the telehealth activity;[14] if you disclose PHI while providing care at a Starbucks, the OCR would probably not think you had made a good-faith effort to protect that information. Providers should be encouraged to select private locations when providing telehealth.

Training should also cover restricting access to the device used to provide services and physical and logical security of the device. Take this opportunity to remind your workforce that leaving laptops unattended in cars or other places is never a good idea. Remember, a laptop is stolen every 53 seconds, and in 2018, 45% of the healthcare information breaches were a result of lost or stolen laptops.[15] This is also a good time to do refresher training on information technology security, including reminders of the risks of phishing.

One new area that you may want to consider is training on the use of patient contact information. While the patient may have given you access to their contact information for the purpose of care delivery, you want to be sure that you don't use that information in violation of other privacy regulations such as the Telephone Consumer Protection Act.[16] While you might think it would be beneficial to send out a recording to all your patients announcing a new location or service, this could expose you to unexpected risks. The act essentially prohibits calls and text messages to residential and wireless numbers using an auto-dialer or prerecorded messages without the recipient's prior consent. In 2015, Walgreens paid an $11 million settlement for sending automated prescription reminder calls without permission.[17]

This document is only available to members. Please log in or become a member.

Become a Member Login

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.