In response to the global Coronavirus (COVID-19) pandemic, US state and federal government agencies have worked to promote utilization of telehealth. Prior to and following President Trump’s declaration of a national emergency related to the COVID-19 pandemic, the HHS Office for Civil Rights has issued bulletins and guidance to help ensure that the provision of telehealth and other services is not inappropriately constrained during the pandemic by HIPAA privacy and security requirements. This On the Subject summarizes key insights, open questions and operational tips related to OCR’s COVID-19 related guidance and opportunities for additional OCR guidance.

IN DEPTH

In response to the global Coronavirus (COVID-19) pandemic, US state and federal
government agencies have worked to promote utilization of telehealth. On March 13, 2020, President Trump issued a Proclamation on Declaring a National Emergency Concerning the Novel Coronavirus Disease (COVID-19) Outbreak (the Presidential Proclamation Concerning COVID-19), providing that the Secretary of the US Department of Health and Human Services (HHS) may exercise authority to temporarily waive or modify certain requirements of the Medicare, Medicaid, and state Children’s Health Insurance programs and the Health Insurance Portability and Accountability Act (HIPAA).

To that end, the Centers for Medicare and Medicaid Services (CMS) have expanded Medicare’s telehealth benefits. Myriad state and federal government agencies, government payors and private payors have expanded reimbursement for telehealth services and loosened professional licensure restrictions to promote implementation. The HHS Office for Civil Rights (OCR) has issued the following bulletins and guidance (collectively, the OCR COVID-19 Guidance) to help ensure that the provision of telehealth and other services during the COVID-19 pandemic is not inappropriately constrained by HIPAA privacy and security requirements:

- OCR, FAQs on Telehealth and HIPAA during the COVID-19 nationwide public health emergency, March 20, 2020 (OCR FAQs 3/20/20)
- OCR, Notification of Enforcement Discretion for telehealth remote communications during the COVID-19 nationwide public health emergency, March 17, 2020 (OCR Notification 3/17/20)

This On the Subject summarizes key insights, open questions and operational tips related to the OCR COVID-19 Guidance and opportunities for additional OCR guidance.

Privacy and Security Compliance Insights and Open Questions

- OCR will not impose penalties for noncompliance with HIPAA against covered entity healthcare providers in connection with the good faith provision of telehealth during the COVID-19 national emergency. Covered entity healthcare providers that want to use remote communication technologies to provide telehealth to patients during the COVID-19 national emergency—even if the telehealth is not related to the diagnosis or treatment of COVID-19—can use any “non-public facing” remote communication products that are available to communicate with patients.

Non-public facing remote communication products would include, for example, in the video application context, Apple FaceTime, Facebook Messenger video chat, Google Hangouts video, Whatsapp video chat and Skype, and, in the text application context, Signal, Jabber, Facebook Messenger, Google Hangouts, Whatsapp and
In OCR Notification 3/17/20, OCR states that, effective immediately, OCR will exercise its enforcement discretion and will not impose penalties for noncompliance with HIPAA against covered entity healthcare providers in connection with the good faith provision of telehealth during the COVID-19 national emergency. OCR specifically states that covered entity healthcare providers that want to use remote communication technologies to provide telehealth to patients during the COVID-19 national emergency—even if the telehealth is not related to the diagnosis or treatment of COVID-19—can use any “non-public facing” remote audio or video communication products that are available—e.g., Apple FaceTime, Facebook Messenger video chat, Google Hangouts video or Skype—to communicate with patients.

This list of remote communication product examples provided in OCR Notification 3/17/20 was not intended to be exhaustive. In the OCR FAQs 3/20/20, OCR provided additional examples of remote communication products to which the enforcement waiver would apply and clarified that they could include text applications and not just audio and video applications. The list was expanded to include, for video applications, WhatsApp video chat, and, for text applications, Signal, Jabber, Facebook Messenger, Google Hangouts, Whatsapp and iMessage. In the OCR FAQs 3/20/20, OCR notes favorably that these applications typically employ end-to-end encryption, support individual user accounts, logins and passcodes to help limit access and verify participants, and/or permit participants to assert some degree of control of particular capabilities, such as choosing to record or not record the communication or to mute or turn off the video or audio at any point.

OCR acknowledges in OCR Notification 3/17/20 that the enforcement waiver extends to failures to enter into business associate agreements with vendors of such non-public facing remote communication products and utilization of non-HIPAA-compliant remote communication products. However, OCR distinguishes the above “non-public facing” remote communication products from “public facing” remote communication products—e.g., Facebook Live, Twitch, TikTok and similar video communication applications—which are not subject to the enforcement waiver and may not be used in the provision of telehealth. OCR notes in the OCR FAQs 3/20/20 that these products are designed to be open to the public or allow wide or indiscriminate access to the communication and, accordingly, a provider that chooses to use such products would not be covered by the enforcement waiver.

The enforcement waiver extends only to covered entities that are healthcare providers and not to covered entities that are health plans or healthcare clearinghouses. OCR made clear in the OCR FAQs 3/20/20 that even health plans that pay for telehealth services are not subject to the enforcement waiver because they are not engaged in the provision of healthcare.

- **OCR encourages providers to notify patients that third-party communications applications potentially introduce privacy risks and to enable all available encryption and privacy modes when using such applications.**

In OCR Notification 3/17/20, OCR encourages covered entity healthcare providers to
notify patients that remote communication products potentially introduce privacy risks and to enable all available encryption and privacy modes when using such products. OCR does not address whether the patient notifications of privacy risks should be in writing and provided prior to a telehealth visit or whether they may be provided orally at the beginning of a telehealth visit. Because OCR is merely “encouraging” and not “requiring” providers to provide such notifications, providers will need to evaluate the feasibility of such notifications and the most appropriate methods of implementation.

- **OCR advises that covered entity healthcare providers that seek additional privacy protections for telehealth should provide such services using vendors that provide HIPAA-compliant remote communication products and that will enter into business associate agreements in connection with the provision of their products.**

While exercising its enforcement discretion as to utilization of non-HIPAA-compliant communication products by covered entity health-care providers for telehealth in connection with the good faith provision of telehealth during the COVID-19 national emergency, OCR also advises that covered healthcare providers that seek additional privacy protections for telehealth should provide such services using vendors that provide HIPAA-compliant remote communication products and that will enter into business associate agreements in connection with the provision of their products. In OCR Notification 3/17/20, OCR provides a non-exhaustive list of vendors that represent that they provide HIPAA-compliant video communication products and will enter into business associate agreements, e.g., Skype for Business, Updox, VSee, Zoom for Healthcare, Doxy.me, and Google G Suite Hangouts Meet. Because OCR is merely advising providers that seek additional privacy protection to utilize such vendors (and not requiring providers to use such vendors), providers will need to evaluate the feasibility of engaging such vendors during the national emergency.

When the national emergency and enforcement waiver described in OCR Notification 3/17/20 terminate—and perhaps even in anticipation of eventual termination—providers that are not utilizing “HIPAA-compliant” remote communication products as described in the OCR COVID-19 Guidance will need to evaluate, inter alia, whether their preferred product vendors are appropriately characterized as “business associates” or as mere “conduits” (in accordance with existing OCR guidance, which distinction is beyond the scope of this article) and/or whether they should transition to “HIPAA-compliant” products and vendors as described in the OCR COVID-19 Guidance.

- **The enforcement waiver described in OCR Notification 3/17/20 does not have an expiration date. OCR will issue an additional notice to the public when it is no longer exercising its enforcement discretion based on then-present facts and circumstances.**

The enforcement waiver described in OCR Notification 3/17/20 does not contain a specific expiration date. Because OCR Notification 3/17/20 states that OCR will not impose penalties for noncompliance in connection with the good faith provision of telehealth “during the COVID-19 nationwide public health emergency,” one might conclude that the enforcement waiver would automatically terminate upon a presidential proclamation that the national emergency declared in the Presidential
Proclamation Concerning COVID-19 has terminated. However, OCR has clarified in the OCR FAQs 3/20/20 that the enforcement waiver would terminate only after OCR issues an additional notice to the public that it is no longer exercising its enforcement discretion based on then-present facts and circumstances. Consequently, the enforcement waiver described in OCR Notification 3/17/20 might theoretically be terminated before or after the national emergency declared in the Presidential Proclamation Concerning COVID-19 has terminated.

- The enforcement waiver described in the OCR COVID-19 Guidance may not extend to non-HIPAA-compliant voicemail applications. Providers should further evaluate utilization of such applications prior to implementation.

The OCR COVID-19 Guidance makes clear that the enforcement waiver extends to non-public facing remote communication products with specific reference to audio, video and text applications. The OCR COVID-19 Guidance does not specifically address voicemail applications. OCR notes in the OCR FAQs 3/20/20 that the products to which it has specifically extended its enforcement waiver typically employ end-to-end encryption, support individual user accounts, logins and passcodes to help limit access and verify participants, and/or permit participants to assert some degree of control of particular capabilities, such as choosing to record or not record the communication or to mute or turn off the video or audio at any point. Voicemail is by its nature a recorded communication, and one of the products listed by OCR states on its website that voice messages are encrypted when they are delivered to the user, but, after the user listens to the message, the voicemail is transferred from the vendor’s servers to the user’s local device where it is stored as an unencrypted file. Because voicemail is not specifically addressed by the OCR COVID-19 Guidance, providers should further evaluate utilization of non-HIPAA-compliance voicemail applications prior to implementation.

- Covered entity healthcare providers may want to consider including non-public facing remote communication products in the scope of their HIPAA security rule risk analyses.

As described above, the OCR COVID-19 Guidance states that OCR will not impose penalties against covered entity healthcare providers for non-compliance with HIPAA requirements in connection with the good faith provision of telehealth services during the COVID-19 nationwide public health emergency. To that end, OCR specifically acknowledges in OCR Notification 3/17/20 that the enforcement waiver extends to failures to enter into business associate agreements with vendors of certain non-public facing remote communication products and utilization of certain non-HIPAA-compliant remote communication products. OCR also makes clear in the OCR FAQs 3/20/20 that it will not impose penalties if electronic PHI (E PHI) is intercepted during transmission while the provider is using one of the non-public facing remote communication products that it describes.

However, OCR does not specifically address whether covered entity healthcare providers must nonetheless include such non-public facing remote communication products within the scope of their HIPAA Security Rule risk analyses and is silent on whether OCR will impose penalties against covered entity healthcare providers for failure to do so. Inclusion of such products within the scope of security risk analyses
would ordinarily be required under the HIPAA Security Rule.

Conducting a security risk analysis is primarily an “internal” process for covered entity healthcare providers. A security risk analysis could be completed by the covered entity healthcare provider in the absence of any affirmative act by the remote communication product vendor and irrespective of the compliance status of the remote communication product or vendor. Because conducting a security risk analysis is different in that respect (i.e., it is primarily an internal process) from executing a business associate agreement with an external remote communication product provider, and because OCR is silent on whether OCR will impose penalties against covered entity healthcare providers for failure to include such products in their security risk analysis, covered entity healthcare providers should consider, notwithstanding the OCR COVID-19 Guidance, including non-public facing remote communication products in the scope of their security risk analyses, with specific consideration of:

- Identifying and documenting reasonably anticipated threats to the confidentiality, availability and integrity of EPHI processed by the product.

- Assessing and documenting the technical, physical and administrative security measures used to safeguard EPHI transmitted through the product, whether security measures required by the Security Rule are already in place and configured and used properly.

- Assessing the likelihood of potential risks and threat occurrences to EPHI.

- Assessing the impact of potential risks to the confidentiality, integrity and availability of EPHI (i.e., the qualitative and/or quantitative magnitude of the potential impact resulting from a threat triggering or exploiting a specific vulnerability).

- Assigning risk levels for all threat vulnerability combinations identified during the risk analysis based on the likelihood of threat occurrence and resulting impact/magnitude.

- Identifying and documenting corrective actions (e.g., new or amended security procedures) to reduce all identified risks to a reasonable and appropriate level. (For example, if the product presents a risk of unplanned downtime during regular patient care hours, the covered entity may wish to reduce that risk by identifying a back-up product and procedures for restoring connectivity with patients.)

- **Covered entity healthcare providers should evaluate the architecture, encryption and functionalities of non-public remote communication products not specifically enumerated in the OCR COVID-19 Guidance prior to utilizing such products.**

The OCR COVID-19 Guidance states that covered entity healthcare providers that want to use remote communication technologies to provide telehealth to patients during the COVID-19 national emergency—even if the telehealth is not related to the diagnosis or treatment of COVID-19—can use any “non-public facing” remote
communication products that are available to communicate with patients. The non-
exhaustive list of such products provided by OCR includes, in the video application
context, Apple FaceTime, Facebook Messenger video chat, Google Hangouts video,
Whatsapp video chat and Skype, and, in the text application context, Signal, Jabber,
Facebook Messenger, Google Hangouts, Whatsapp and iMessage.

The OCR COVID-19 Guidance also provides a non-exhaustive list of technologies that
it considers “public-facing” and therefore not covered by the scope of its
enforcement waiver. These include Facebook Live, Twitch and TikTok.

Accordingly, covered entity healthcare providers should evaluate carefully whether
products that do not appear in OCR’s list of permitted examples of “non-public
facing” products are actually “public” facing or “non-public” facing and whether they
include security measures utilized by one or more of the specifically permitted non-
public-facing products (e.g., employing end-to-end encryption, supporting individual
user accounts, logins and passcodes to help limit access and verify participants,
and/or permitting participants to assert some degree of control of particular
capabilities, such as choosing to record or not record the communication or to mute
or turn off the video or audio at any point).

Provider Operational Tips and Patient Considerations

Many patients may not have experience using remote communications products and
may need guidance on how to use them as securely as possible. This is particularly
important for products that have patient-facing components on patient-controlled
devices (e.g., smart phones) because the security settings and practices in the
patient environment may impact the assessment of the benefits and risks of using
such products. Accordingly, we have included examples of additional steps that
covered entities may wish to consider implementing:

- **Covered entity healthcare providers should implement reasonable
  safeguards to prevent incidental disclosures of PHI during telehealth
  visits, including, for example and without limitation, adopting policies
  and procedures regarding provider participation in telehealth visits from
  private locations where the visit may not be viewed or overheard by
  unauthorized persons.**

The HIPAA Privacy Rule provides that covered entities must reasonably safeguard
PHI to limit incidental uses or disclosures of PHI made pursuant to an otherwise
permitted or required use or disclosure. A commonly cited example of such
incidental uses and disclosures is oral disclosures among providers in public or
semi-private treatment settings (e.g., a nurses’ station). The requirement to
implement reasonable safeguards to limit such disclosures continues to apply in the
telehealth visit context because OCR has not expressly waived enforcement of this
requirement in the OCR COVID-19 Guidance.

In fact, OCR states in the OCR FAQs 3/20/20 that providers should always use
private locations and that patients should not receive telehealth services in public
or semi-public settings, absent patient consent or exigent circumstances, and that,
if telehealth cannot be provided in a private setting, covered entity healthcare
providers should continue to implement reasonable safeguards to limit incidental
uses and disclosures of PHI. Consequently, covered entity healthcare providers should implement reasonable safeguards to prevent incidental uses and disclosures of PHI during telehealth visits, including, for example and without limitation, adopting policies and procedures regarding provider participation in telehealth visits from private locations and when and whether patient consent should be obtained under exigent circumstances for telehealth visits from non-private locations. Such policies and procedures should cover, where applicable, provider participation in telehealth visits from the regular practice location, from home and semi-private locations.

- **Covered entity healthcare providers should evaluate and implement processes for onboarding and engaging patients in the telehealth visit process in compliance with HIPAA and other applicable requirements.** This process might include, for example and without limitation, written or oral communications to patients regarding telehealth visit scheduling, instructions for downloading relevant mobile applications, and transmissions and acknowledgements of receipt of notices of privacy practices.

Covered entity healthcare providers may face operational and communications challenges in connection with onboarding and engaging patients in the telehealth visit process. This process might include, for example and without limitation, written or oral communications to patients regarding telehealth visit scheduling, instructions for downloading relevant mobile applications, and transmissions and acknowledgements of receipt of notices of privacy practices.

To the extent such communications are transmitted via unencrypted email, OCR’s existing guidance regarding unencrypted email would likely apply. (See, for example, the OCR FAQ, “[Does the HIPAA Privacy Rule permit health care providers to use e-mail to discuss health issues and treatment with their patients?](https://www.hhs.gov/ocr/privacy/hipaa/faq/index.html#email)” Specifically, in accordance with this guidance, covered entity healthcare providers should evaluate the application of safeguards to reasonably protect the privacy and security of PHI transmitted via unencrypted email, including limiting the amount or type of information disclosed through unencrypted e-mail, and evaluate the need to advise patients of the risks of communication via unencrypted email. In addition, covered entity healthcare providers should ensure that any unencrypted email transmissions are otherwise in compliance with the HIPAA Privacy and Security Rules (including the rights of individuals to request methods of communication), the CAN-SPAM Act and other requirements.

To the extent such communications are transmitted to patients via SMS message or mobile device notification, covered entity healthcare providers should ensure that such transmissions comply with the HIPAA Privacy and Security Rules (including the rights of individuals to request confidential methods of communication), the Telephone Consumer Protection Act and other requirements.

The OCR COVID-19 Guidance also notes the need to explain to patients the risks and benefits of using non-HIPAA-compliant non-public-facing remote communication products. Covered entities may want to consider developing talking points to help patients appropriately balance risks to privacy against other important needs.
Healthcare providers may also want to explain to patients the steps that patients can take to safeguard their privacy if the telehealth technology involves the use of mobile device applications or other stored solutions on patient-controlled devices. For example, patients could be advised to reset passwords, improve password strength or shorten the time that a device can be idle before the device locks. If the remote communications product leverages photos (e.g., of a wound) or videos (e.g., of someone coughing or stumbling), patients could be advised about how to remove such images from their phones after the consult.

- **Covered entity healthcare providers that conduct telehealth visits with more than one person in the same telehealth “session” (e.g., a healthcare provider conducts a telehealth visit with a person, the person’s spouse and/or the person’s child during the same call or video session) should ensure timely, separate and accurate documentation in each person’s EMR.**

Covered entity healthcare providers should take care to timely and accurately document telehealth visits in the appropriate EMR. To the extent that providers conduct telehealth visits remotely, covered entities should evaluate the provision of remote access to applicable EMR systems in accordance with HIPAA for this purpose or otherwise ensure they have implemented policies, procedures and processes for the timely documentation of such visits. In addition, to the extent providers may visit with more than one patient during a single telehealth call or video session, providers should ensure that relevant information is documented in the record of the applicable patient to avoid potential compliance concerns and breaches of PHI.

- **In addition to evaluating the HIPAA privacy and security operational considerations identified above, covered entity healthcare providers should evaluate third party payor reimbursement considerations in the telehealth context.**

The enforcement waiver described in the OCR COVID-19 Guidance does not itself expand obligations of payors to reimburse for telehealth services. In fact, the OCR FAQs 3/20/20 specifically cautions providers that for purposes of reimbursement, certain payors, including Medicare and Medicaid, may impose restrictions on the type of technologies that can be used. For more information on the topic of reimbursement for telehealth during the COVID-19 national emergency, please visit the Health Law section of McDermott’s Coronavirus Resource Center.

- **Covered entity healthcare providers that are substance use disorder treatment providers within the meaning of 42 C.F.R. Part 2 (Part 2) should evaluate whether more restrictive non-disclosure requirements continue to apply.**

The Substance Abuse and Mental Health Services Administration (SAMHSA) provided guidance on March 19, 2020 (SAMHSA Guidance 3/19/20), in response to the COVID-19 pandemic to help ensure that substance use disorder treatment services are not interrupted by the public health emergency and acknowledging an increased need for telehealth services. The SAMHSA Guidance 3/19/20 states that Part 2’s requirements to obtain written patient consent for disclosure of substance use disorder records would not apply to utilization of telehealth services to the extent that, as
determined by the provider, a medical emergency exists. This “medical emergency”
exception may be narrower than the enforcement waivers described in the OCR
COVID-19 Guidance, so substance use disorder treatment providers should continue
to evaluate disclosures of treatment information in the Part 2 contents and whether
the medical emergency exception is satisfied.

Opportunities for Additional OCR Guidance

Based on our review of the OCR COVID-19 Guidance and feedback from front-line
covered entity healthcare providers, the following additional guidance from OCR
could be helpful in the context of telehealth and the COVID-19 nationwide public
health emergency:

- OCR could clarify that the enforcement waiver described by the OCR COVID-19
  Guidance extends to failures by covered entity healthcare providers to consider
  non-public facing remote communication products within the scope of their
  HIPAA Security Rule risk analyses in connection with the good faith provision of
  telehealth during the COVID-19 nationwide public health emergency.

- OCR could clarify that the enforcement waiver described by the OCR COVID-19
  Guidance extends to transmission of unencrypted email communications by
  covered entity healthcare providers to patients regarding product onboarding,
  telehealth visit scheduling and utilization in connection with the good faith
  provision of telehealth during the COVID-19 nationwide public health
  emergency.

- OCR could waive enforcement of the Privacy Rule requirement to provide a
  notice of privacy practices to patients and obtain an acknowledgement of
  receipt as to any covered entity healthcare provider in connection with the good
  faith provision of telehealth during the COVID-19 nationwide public health
  emergency. OCR has issued such a waiver in OCR Bulletin 3/16/20 as to
  “covered hospitals” under certain circumstances but not as to other types of
  healthcare providers. Such a waiver would expedite and streamline the
  provision of telehealth services, particularly as to covered entity healthcare
  providers and patients that do not have secure or HIPAA-compliant means of
  electronic transmissions of such notices or acknowledgements of receipt.

© 2020 McDermott Will & Emery

Source URL: https://www.natlawreview.com/article/ocr-enforcement-waivers-
certain-hipaa-requirements-furtherance-telehealth-during