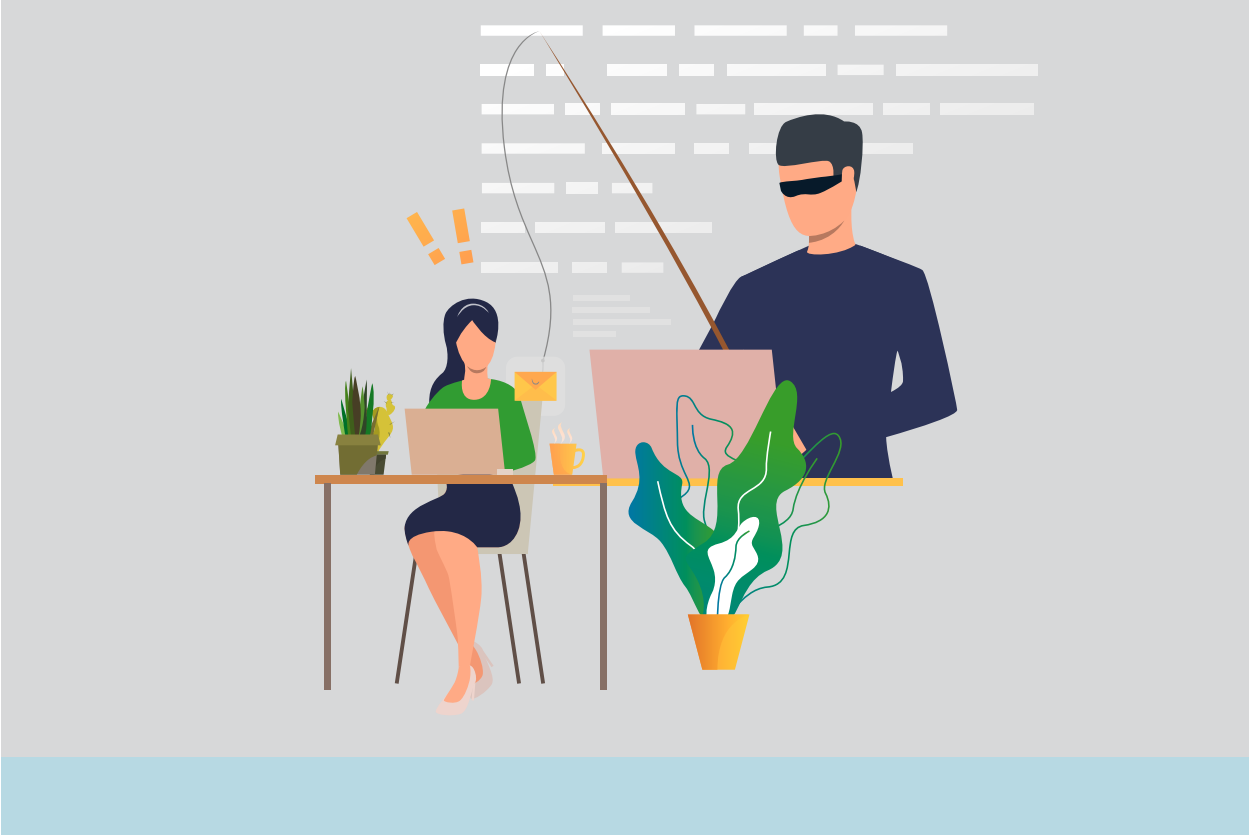
Protecting and Safeguarding Electronic Protected Health Information



MICA®
RISK TEAM

Between 2009 and 2022, health care data breaches have exposed more than 385 million patient records. These breaches include closed cases and breaches that are still being investigated by the Office for Civil Rights for potential HIPAA violations. The Risk Team at the Mutual Insurance Company of Arizona® (MICA) created this resource to help practices stay informed of risk mitigation strategies when protecting sensitive patient data.

This resource provides guidance and examples of protecting electronic protected health information (ePHI), including:

- How to properly dispose of devices that contain ePHI
- What to include when implementing an e-communications policy and procedure for your practice
- What you need to know about HIPAA compliance regarding tracking technologies on your website

About The Risk Team

The Risk Team offers a collaborative approach to managing medical professional liability risk with educational resources and guidance. Our team of Risk Consultants are ready to answer your calls and emails about liability risk such as regulatory requirements, managing conflict, office policies and processes, and other pain points. When you need assistance, the Risk Team will be there for you so you can focus on patient care.

MICA members can contact the Risk Team to schedule a virtual or onsite risk assessment, ask for a resource or request other guidance at 800-705-0538 or rm_info@mica-insurance.com.

Interested in learning more about the benefit of MICA? Visit our website or call us at **800-681-1840.**

Disposal of Devices Containing Electronic Protected Health Information

You wouldn't throw stacks of paper medical records in the trash without shredding them first, but when it's time to dispose of computers, disks, or thumb drives containing patients' electronic protected health information ("ePHI"), do you know what HIPAA requires? The HIPAA Privacy Rule mandates that covered entities ("CEs") implement reasonable safeguards to protect against prohibited uses or disclosures of protected health information ("PHI").[1] CEs must take the same care to protect ePHI, even at the time of disposal. Failure to take steps to properly remove ePHI from electronic devices, prior to reuse or disposal of those devices, is a violation of the HIPAA Security Rule and could result in a data breach.

To avoid hefty penalties for HIPAA noncompliance, and potentially higher costs of a data breach, practices need appropriate policies and procedures governing disposal or reuse of devices containing ePHI. The following summary of HIPAA Security Rule requirements can help you identify compliance gaps.

The HIPAA Security Rule

All ePHI created, received, maintained, or transmitted by a CE is subject to the Security Rule. Covered entities are required to implement reasonable and appropriate security measures to:

- Ensure the security and integrity of ePHI,
- Guard against "reasonably anticipated threats" to ePHI that could compromise its security and integrity, and
- Protect against prohibited disclosures of ePHI that could be "reasonably anticipated."[2]

One risk to ePHI security involves disposal and reuse of electronic devices. For example, if that laptop you donated to charity makes its way into the wrong hands, your patients could end up victims of identity theft if you failed to remove ePHI before donating. To protect against this risk of unauthorized disclosure, CEs are required to implement policies and procedures governing disposal and reuse of electronic devices. HIPAA disposal regulations apply to any device capable of storing ePHI including laptops, desktops, tablets, mobile phones, portable hard drives, zip drives, backup tapes, CDs, or DVDs.

Inventory and Track Your Electronic Devices - The Security Rule "Device and Media Controls Standard"

To avoid inadvertent disposal or reuse of devices containing ePHI, you first need to know where your ePHI is stored. **This involves tracking the movement of all hardware and electronic media into, out of, and within your medical practice as required by the Security Rule's *Device and Media Controls standard.*** This standard requires CEs to implement written policies and procedures governing the "receipt and removal of hardware and electronic media" containing ePHI. "Electronic media" is defined as "electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card."[3]

Disposal of Hardware or Electronic Media Containing ePHI

Your disposal policies and procedures must specify that ePHI will be rendered **unusable or inaccessible prior to disposal** of hardware or media. According to the U. S. Department of Health and Human Services ("HHS"), any of the following methods are acceptable:

- Degaussing, a technique requiring special equipment and uses a strong magnetic field to fully erase data;
- Destruction, which involves damaging the hardware or media beyond repair (disintegrating, pulverizing, melting, incinerating, shredding); and
- Clearing, by using software or hardware to overwrite media with non-sensitive data[4]

In addition to methods to prevent use or access to hardware and electronic storage media, practices should also implement safeguards for disposing of equipment such as printers, copiers, and fax machines. Many of these store data on internal hard drives.

Reuse of Electronic Media Containing ePHI

CEs must put in place policies and procedures governing reuse of electronic media. A medical practice may reuse media internally by, for example, sharing disks or flash drives. The practice might also donate electronic media to charities or schools. In these situations, CEs must delete or make inaccessible all ePHI previously stored on the media to prevent unauthorized access to the data.[5]

Action Plan for Compliance

- Develop a written PHI/ePHI disposal policy as part of their Security Rule policies and procedures.
- Provide and document appropriate training to supervisors and staff who will be implementing these processes.[6]
- Keep training records and copies of retired policies and procedures for at least 6 years.[7]
- When contracting with business associates ("BA") to handle disposal/reuse of electronic media, obtain a signed, HIPAA-compliant BA agreement.[8] Only competent IT personnel (either in-house or contracted BAs) should handle removal of ePHI from hardware/media. Once removal is complete, the date should be entered on your hardware and electronic media log.

Consider including the following in your Device and Media Controls and ePHI Disposal policies and procedures:

- A process for maintaining a log to inventory and track the movement (into, out of, within your practice) of hardware and electronic media containing ePHI.
- A list of the types of hardware and electronic media that must be tracked.
- A procedure to ensure that ePHI is removed prior to disposal.
- A process to permanently delete ePHI or make it inaccessible prior to reusing electronic media.
- A process to safeguard devices/media scheduled for ePHI removal and awaiting pickup by your contracted vendor (e.g., place in a locked cabinet or bin).

Managing e-Communications Risk

The convenience of text, e-mail, and other electronic messaging solutions ("e-communications") can easily overshadow their risks. Inappropriate use of e-communications can result in gaps in medical record documentation and HIPAA violations that come with sizeable penalties.

Implementing an e-communications policy and procedure to manage your risks can reduce the likelihood of regulatory actions and medical professional liability lawsuits. If you're feeling unsure about what to include in a policy, the following guidance and examples may help.

HIPAA Basics

- The HIPAA Privacy and Security Rules require covered entities to secure and protect patients' electronic protected health information ("ePHI") from unauthorized access, whether ePHI is "at rest" (stored electronically in an EHR or saved email, for instance) or "in transmission" (sent electronically to a patient or third party).
- If you contract with a vendor to create, transmit, or maintain ePHI on your behalf, HIPAA obligates you to ensure that the vendor is appropriately securing and protecting the ePHI as well. A Business Associate Agreement ("BAA") is required to confirm this commitment. Examples of vendors that must sign BAAs include cloud service providers or messaging applications that encrypt and store emails or texts containing ePHI.[9]
- When sending e-communications containing ePHI, secure transmission is necessary for HIPAA compliance. This generally requires:
  - encryption or
  - access controls (such as the login required with patient portals).
- If you elect not to use encryption to protect the confidentiality, integrity, and availability of ePHI, HIPAA requires you to maintain documentation for 6 years about the reason for your decision. In any enforcement action or compliance audit, investigators will evaluate compliance by requesting documentation showing:
  - you conducted the required HIPAA Security Rule risk assessment,
  - you developed a risk management plan to address the identified risks,

- you determined that encryption was not a "reasonable and appropriate safeguard" to protect ePHI, and
- your rationale for choosing another equally effective safeguard (or no safeguard at all).[10]

- Text (or SMS) messages are generally not secure.[11] Texts travel unencrypted over the open internet so content is viewable by mobile carriers and other third parties and can be intercepted by hackers.
- Messages sent through free, internet-based e-mail services (Gmail, Hotmail, Yahoo, etc.) are not secure either. In 2012, a small cardiology practice with offices in Phoenix and Prescott paid $100,000 to settle an enforcement action alleging multiple HIPAA violations including:
  - Employees used Internet-based email accounts (personal and business) to exchange emails containing ePHI; and
  - The practice did not have a signed BAA with the Internet-based email provider.[12]
- Patients can waive their right to have ePHI sent securely. A patient may send you an unsecure email or text message containing ePHI and request that you respond. Your obligation to protect ePHI against unauthorized uses and disclosures is triggered when you receive this text or email. For patient waiver of protections to be effective, HIPAA requires that you:
  - warn the patient of unsecured text/email risks;
  - obtain the patient's consent to unsecure communications; and
  - document your warning and the patient's authorization to continue.[13]

  You do not need to repeat this process each time you communicate electronically with the patient – just the first time.

Examples

e-Communications with Patients

1. The patient asks her dermatologist, *"Can I text you pictures of how my skin looks after I've used the medication for a week?"*
   - If the patient's consent is not already documented in the medical record, the dermatologist should follow the warning/consent procedure described above.
     - Better solution: Ask the patient to send the pictures securely through the practice portal.

2. A patient leaves a voice message for his surgeon, requesting a call back – he has questions about his recent procedure and the post-procedure instructions. The busy orthopedic surgeon doesn't get a chance to return the call during office hours, so that night she responds via email from her home computer. She discusses her operative findings and clarifies post-procedure instructions.

    - The physician must ensure the patient consents to unsecure email transmissions before using her internet-based home email to communicate.

        - Better solution: Send an encrypted email through the practice's secure email platform.

        - Best solution: Call the patient (patient requested a call, and live conversation is likely better because of the detail and complexity of the conversation and in case the patient has questions).

E-communications with Non-Patients

1. The practice's biller texts the nurse practitioner ("NP") with questions about patient charges. The text contains the patient's name and date of birth. The NP responds with the requested information.

2. The cardiologist needs more information about the reason for the attending physician's consult request, so he uses his personal Gmail account to email the attending. His message includes the patient's name and other ePHI and is addressed to the attending's personal Hotmail account.

    - Neither communication adequately protects the ePHI. One involves an unencrypted text message and the other involves internet-based personal email accounts.

    - Only patients can waive HIPAA's ePHI protections and agree to unsecure transmissions of their ePHI.

    - Your e-communications policy and procedure should prohibit clinicians and staff from sending or responding to *non-patient* (vendors, clinicians, other third parties) unsecured text/email messages containing ePHI.

    - Provide a copy of your policy to practice vendors that have access to ePHI, such as billing companies.

Chat Applications

The primary care physician works out of her home and provides care via telemedicine or mobile visits to patients' homes. Some patients send her prescription refill requests and other communications via Facebook messaging or WhatsApp.

- Neither application should be used for communications containing ePHI. Although both offer encryption, they may not meet other Security Rule requirements such as integrity and audit controls that protect against improper destruction of ePHI. It is also questionable whether either company would sign a BAA.

Appointment Reminder Texts

The practice scheduler sends the patient the following reminder text: *"Hi Karen Jones. You are scheduled for your well woman exam on August 15, 2022."*

- Eliminate ePHI from scheduling reminder texts: *"Hi Karen. Your appointment with Dr. Jones is this Thursday."*

Other Risks of e-Communications

Mobile Devices

Using mobile devices to store or transmit ePHI increases the risk of data breaches. Mobile devices are vulnerable to attack in the following ways:

- An unsuspecting user accidently downloads malicious software disguised as games, patches, or utilities;
- An unsuspecting user inadvertently visits a malware website disguised as a legitimate website and the site downloads malware to the user's device;
- Hackers intercept communications to and from the user's device; or
- Hackers access information on a lost or stolen device.[14]

If you're using a mobile device for patient-care related activities, the Office of the National Coordinator for Health Information Technology (ONC) recommends that you implement a written Mobile Device policy that incorporates risk assessment and management and provides employee training on privacy and security awareness. Click here for ONC's tips on protecting and securing ePHI on mobile devices.

Documentation

Implement a procedure to ensure that **all** e-communications, however brief, are saved to the medical record. Including these communications in the record:

- Promotes continuity of patient care;

- Preserves all care conversations in case the patient wants to access or amend his/her record;
- Saves essential evidence of all communications to defend against lawsuits or licensing board complaints and investigations; and
- Ensures you can respond to a subpoena for "all electronic communications" about the patient, even in cases where you're not a defendant.

HIPAA Compliance and Your Practice Website

Your medical practice might be using cookies, pixels, or embedded codes (collectively "tracking technologies") on your practice website, which could be a HIPAA violation. Some practice websites are even creating breach situations if the site's tracking technologies collect and share patient data with third parties. Read on to find out about tracking technologies, HIPAA compliance, and avoiding liability for unauthorized disclosures of protected health information.

What are Tracking Technologies?

Businesses in various industries install cookies, pixels, hidden codes, and other tracking technologies on their websites or mobile apps to monitor online visitors' activity. As the user navigates the site, tracking technologies collect data about the user. Some businesses use this data internally to evaluate website traffic or improve website functionality. They also may use it to target visitors with online advertising. Although some organizations develop their own trackers and analyze the data, most businesses contract with a technology vendor to supply the tracker.

The Meta (formerly Facebook) Pixel is one example of a third-party tracking technology. The pixel is a hidden code that tracks users as they navigate through a website, recording which pages they visit, buttons they click, and information they type into forms. It sends this information to Facebook. Using scripts running in a person's internet browser, it labels each packet of data sent to Facebook with a unique IP address (like a computer's mailing address) that can be used to identify an individual or household.[15] If you saw an ad on your Facebook feed for a retailer, health care provider, or other business whose website you recently visited, that was Meta Pixel at work.

Don't Assume Tracking Technologies Aren't on Your Practice Website or Sharing Patient Information

In June 2022, *The Markup* published an article revealing that Meta Pixel was embedded on one-third of the hospital appointment scheduling webpages it reviewed and was sending patients' sensitive health information to Facebook. For example, when a patient clicked "Schedule Online" on one hospital's webpage, Meta Pixel sent Facebook information including the doctor's name and the diagnosis/condition entered by the patient (e.g, "Alzheimers" or "pregnancy termination").

Clicking the "Finish Booking" button on another page prompted Metal Pixel to send the name of the doctor, the doctor's medical specialty, and the patient's first name, last name, email address, phone number, zip code, and city of residence. *The Markup* found the pixel installed **inside** password-protected portals on seven websites. Data shared with Facebook included details about patients' medications and upcoming doctor's appointments. *The Markup* says that many of the hospitals removed Meta Pixel from their sites after it shared its findings with them.

The article's publication prompted hospitals and other organizations to investigate exactly what data their website trackers were collecting and sharing.[16] For example, Community Health Network ("Community") announced that it launched an investigation into its own data tracking practices and hired a third-party forensic team. The organization said, "Th[e] investigation confirmed that third-party tracking technologies were installed on Community's website, including the MyChart patient portal and on some of the appointment scheduling sites."[17] Community said it did not realize the extent of patient information that was being collected and transferred to third parties.[18]

As a result of internal investigations, like the one conducted by Community, many hospital systems had to report data breaches stemming from their own use of Meta Pixel and other tracking technologies. Then, in late 2022, several that made breach reports were slapped with class action lawsuits filed by patients whose information was sent to third parties like Facebook.[19]

The lesson to be learned from these events is that you could be in the same boat, even if you're a small physician practice. Tracking technologies are often used as marketing tools. A vendor designing and managing your website may install software containing pixels that collect and share data without your knowledge.

In light of new guidance (discussed below) issued by HHS, it's important to know for sure. The first step in avoiding regulatory investigations, fines, and penalties is to assess whether and how your website is using tracking technologies.

OCR Issues Guidance to HIPAA Covered Entities Using Tracking Technologies

Six months after The *Markup* article was published, the HHS Office of Civil Rights ("OCR") issued Guidance cautioning HIPAA covered entities ("CEs") and business associates about the use of tracking technologies. In the Guidance, OCR takes the broad position that **all** individually identifiable health information ("IIHI")[20] a tracker collects on a CE's website or app "generally is PHI" and thus protected from improper disclosure by the Security and Privacy Rules.[21] According to OCR, such information might include medical record numbers, home or email addresses, dates

of appointments, an IP address or geographic location linked to the individual, medical device IDs, or any unique identifying code. OCR considers this the case even when the individual and CE do not have an existing relationship or the IIHI does not contain specific treatment/billing information. OCR's rationale is that collection of IIHI through an entity's website/app creates a connection between the individual and the CE because it indicates the CE will provide services to the individual and relates to the individual's past, present, or future health, health care or payment for care.

Trackers on authenticated and unauthenticated pages of a CE's website

The Guidance cautions that trackers on authenticated webpages (which require users to log in), requiring user login, such as patient portals or telehealth platforms, likely access PHI in the form of addresses, appointment dates, IP addresses and potentially even diagnoses, prescriptions, or treatment, or billing information. OCR confirms that if tracking technologies do not access PHI, then HIPAA Rules do not apply. This could be the case on unauthenticated webpages (no log in requirement) where the CE merely offers general information about location, policies and procedures, or services provided. OCR cautions, however, that trackers on some unauthenticated pages do collect PHI and includes the following examples in the Guidance:

- *Portal login page or pages where user registers for a portal account* – If the page requires login or registration information, and a tracker collects data such as credentials, name, or address, this is PHI and HIPAA applies.
- *Provider availability/appointment scheduling pages* – On some unauthenticated webpages a tracker may collect PHI, such as an email or IP address, when the individual searches for available appointments with a provider.

HIPAA compliance when using trackers

CEs and business associates using tracking technologies should incorporate the following guidance from OCR[22] into their compliance programs:

Privacy Rule

- Ensure the Privacy Rule permits disclosure[23] **and** the CE has a signed business associate agreement ("BAA")[24] in place with the vendor **before** disclosing any PHI to technology vendors, mobile app vendors, or other third parties.
- **If** the Privacy Rule permits disclosure, unless an exception applies, restrict the disclosure to include only the minimum necessary PHI to achieve the intended purpose.

- CEs must evaluate whether the vendor meets HIPAA's definition of a "business associate"[25] before asking for a signed BAA. If a vendor does not fall within the definition, a signed BAA is worthless.
- The BAA must list the vendor's permitted and required uses and disclosures of PHI.
- The BAA must require the vendor to safeguard the PHI and report any security incidents (including breaches of unsecured PHI) to the CE. According to OCR, "It is insufficient for a tracking technology vendor to agree to remove PHI from the information it receives or de-identify the PHI before the vendor saves the information."
- Some web tracker vendors or other third parties will not sign BAAs. In this case, even if the vendor meets the business associate definition and the Privacy Rule permits the PHI disclosure, the CE must obtain a signed HIPAA authorization from the individual prior to sharing data with the vendor.
- CEs may mention their use of tracking technologies in privacy policies, notices, or terms/conditions of use on a website or app. However, this does not cancel the CE's obligation to obtain a BAA and ensure a Privacy Rule permissible purpose prior to disclosing PHI to third parties.
- Where there is not an applicable Privacy Rule permission (e.g., disclosure is for marketing purposes) or there is no BAA, a CE must obtain a HIPAA-compliant authorization from the individual before disclosing PHI to a vendor or other third party. A website banner that asks users to accept/reject the use of cookies or other web tracker **does not** substitute for a signed, valid HIPAA authorization.

Security Rule

- CEs and BAs must address the use of tracking technologies in the Risk Analysis and Risk Management processes required by the Security Rule.[26]
- CEs/BAs must implement administrative, physical, and technical safeguards to secure information collected by trackers, including encrypting ePHI during transmission and enabling and using appropriate authentication, access, encryption, and audit controls to protect ePHI the vendor maintains.

Breach Notification

- When a CE discloses PHI to a tracking technology vendor in violation of the Privacy Rule, and the CE cannot demonstrate a low probability the PHI was comprised, the Breach Notification Rule[27] applies. In this case, the CE must notify affected individuals, the Secretary of HHS, and, if applicable, prominent area media outlets.

Steps to Take Now

Going forward, physician practices and other CEs should meet with their marketing and/or IT personnel or vendors to determine if there are tracking technologies on the practice website. If your practice uses tracking technologies, it is critical to:

- understand exactly what information is collected on what webpages and what happens to that information;
- develop a plan to ensure your use of trackers complies with the OCR guidance discussed above;
- confirm appropriate BAAs are in place;
- modify your Security Rule Risk Analysis and Risk Management findings; and
- consult legal counsel to understand what practices may be prohibited, develop a compliance plan to mitigate potential liability for improper data sharing, and determine if you have breach reporting obligations.

Endnotes

1 45 CFR § 164.502; https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

2 45 CFR § 306(a)(1)-(3); https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.

3 45 CFR § 164.310(d)(1); https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf.

4 45 CFR § 164.310(d)(2)(i); https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf.

5 45 CFR § 164.310(d)(2)(ii); https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf.

6 45 CFR § 164.530(b)(1)-(2).

7 45 CFR § 164.530(b)(2)(ii) & (j)(1)-(2) & 164.316(b)(1) & (2)(i).

8 45 CFR § 164.314(a)(1)-(2); https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html.

9 https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html

10 *See* 45 CFR § 164.312(a)(2)(iv) (e)(2)(ii). See also https://www.hhs.gov/hipaa/for-professionals/faq/2001/is-the-use-of-encryption-mandatory-in-the-security-rule/index.html.

11 For a secure method of sending texts, consult your IT team about the availability of secure messaging platforms that provide encryption, limit access, and offer other security measures required by HIPAA.

12 https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/enforcement/examples/pcsurgery_agreement.pdf

13 Semel, M. (2018 March 6). Texting patients is ok under HIPAA, as long as you…. *Healthcare IT Today* (*citing* remarks by HHS Director Roger Severino during a speech at the March 2018 HIMSS health IT conference). https://www.healthcareittoday.com/2018/03/06/texting-patients-is-ok-under-hipaa-as-long-as-you/. Although the U.S. Department of Health and Human Services says you can assume a patient consents to the security risks if he/she initiates the email or text communication, the least risky practice is to document warning and consent anyway. https://www.hhs.gov/hipaa/for-professionals/faq/570/does-hipaa-permit-health-care-providers-to-use-email-to-discuss-health-issues-with-patients/index.html#:~:text=Yes.,See%2045%20C.F.R.

14 https://www.healthit.gov/faq/what-are-some-activities-make-mobile-devices-vulnerable-attack

15 Feathers, T., Fondrie-Teitler, S., Waller, A., & Mattu, S. (June 2022), Facebook is receiving sensitive medical information from hospital websites. *The Markup*. https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites.

16 *Id.*; *see also* Fox, A. (2022, December), Community Health Network reports online tracking data breach affecting 1.5 million. *Healthcare IT News*. https://www.healthcareitnews.com/news/community-health-network-reports-online-tracking-data-breach-affecting-15-million

17 Fox, A. (2022, December), Community Health Network reports online tracking data breach affecting 1.5 million. *Healthcare IT News*. https://www.healthcareitnews.com/news/community-health-network-reports-online-tracking-data-breach-affecting-15-million

18 *Id.*

19 *Id.*; Muoio, D. & Burky, A. (November 2022), Advocate Aurora, WakeMed get served with class action over Meta's alleged patient data mining. *Fierce Healthcare*. https://www.fiercehealthcare.com/health-tech/report-third-top-hospitals-websites-collecting-patient-data-facebook#:~:text=Advocate%20Aurora%2C%20WakeMed%20get%20served,Meta's%20alleged%20patient%20data%20mining&text=Facebook%20parent%20company%20Meta%20is,hospital%20and%20patient%2Dfacing%20websites.

20 IIHI is generally a subset of health information collected from an individual, including demographic information, that is created or received by a CE (or its business associate), relates to an individual's past, present, or future health condition, health care, or payment for health care, and identifies or can be used to identify the individual. 45 CFR § 160.103.

21 HHS, Use of Tracking Technologies by HIPA Covered Entities and Business Associates. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

22 *Id.*

23 *See* 45 CFR § 164.502(a)(1) regarding permissible disclosures.

24 HHS offers guidance and a model agreement at https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html.

25 45 CFR §160.103 (business associate definition). For more information about business associates see https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html.

26 HHS offers guidance on compliance with the Security Rule at https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html?language=es.

27 45 CFR §§ 164.400-414.