SheppardMullin

Hot Topics in HIPAA

2025

Table of Contents

SheppardMullin

About the Author

Michael Sutton
Associate
469.391.7455 | msutton@sheppardmullin.com

Full Bio

Michael Sutton is an associate in the Healthcare Industry Team at Sheppard Mullin's Dallas office, specializing in healthcare privacy, digital health, and data usage. As a member of the Digital Health Team and lead associate for the Health-e Law podcast, Michael guides clients through operational matters in the digital health and healthcare privacy spaces, supporting resolution of breaches, negotiation of data ownership and usage rights, development of comprehensive compliance programming, while also navigating compliance with emerging challenges such as artificial intelligence, telehealth, offshoring, derivative use of data, and other next-gen workstreams.

Five Quick Fixes for Compliance

1. Modernize Your NPP

THE ISSUE

As public-facing representations, inaccurate Notices of Privacy Practices ("NPP") can provide a basis for deceptive or unfair trade practices or unfair competition claims, including under the FTC Act. In fact, class actions and enforcement actions are on the rise, many of which cite representations in NPPs as grounds for substantial damages, with recent judgments and settlements ranging into the millions of dollars.

THE FIX

Review your organization's NPP to ensure it is consistent with your organization's current operations as well as with recent laws and regulations.

2. Sanitize Your Social Media

THE ISSUE

HIPAA generally prohibits use and disclosure of health information on social media without the patient's consent. Issues may arise where a regulated party posts pictures or testimonials which identify patients, or where regulated parties respond to patient reviews. Even something as seemingly innocuous as acknowledging a patient review or thanking a patient for his/her review, without more, could constitute a violation of HIPAA.

THE FIX

Review your organization's social media accounts to identify patient engagement which may violate HIPAA. Consider removing all explicit patient interactions unless patient consent is clearly documented, as well as implementing policies and procedures to govern use of social media across an organization.

3. Check Your Website for Trackers

THE ISSUE

Tracking technologies, such as analytics tools and pixels, often prove tremendously helpful by providing insight as to user traffic, interest, and engagement. These technologies have been accompanied by a sharp increase in class action lawsuits and regulatory enforcement actions specifically targeting use of third-party tracking technologies on healthcare websites.

THE FIX

Check your organization's website to identify use of tracking technologies. If such technologies are detected, take steps to ensure that you have implemented the appropriate compliance measures as well as that use of such technologies is consistent with your organization's posted privacy policies. Consider disabling such technologies until all necessary compliance measures are in place.

4. Feed Your AI Good Data

THE ISSUE

AI is data hungry. This is particularly true as AI is ordinarily trained on large pools of data. It is vital that your organization ensures that it maintains the appropriate rights and licenses to use data, including patient data, which is derived from third parties.

THE FIX

Review your organization's use of AI to determine whether it is processing health information. Consider adopting policies and procedures which limit use of AI tools to process health information without appropriate approvals and controls.

5. Secure Your Texts and Emails

THE ISSUE

HIPAA requires regulated parties to safeguard health information, including when communicating with patients. HIPAA generally prohibits communication of health information through unsecure means, which can include text messages and emails, which could trigger a HIPAA violation. Beyond HIPAA, texting and emailing can implicate other authorities, such as the TCPA and CAN-SPAM Act.

THE FIX

The safest tactic is to ask patients for consent to text or email communications. In addition, take steps to reduce security-related risks, such as by verifying the patient's number or email to ensure accuracy while also limiting the content of messages to non-sensitive matters.

DEEPER DIVE

There have been several notable changes to HIPAA and related privacy laws in recent years, including most significantly:

- Privacy Challenges for Artificial Intelligence
- Additional Protections of PHI Regarding Reproductive Health Care
- Recognizing Your Data as an Asset
- Health Care Needs More Hackers
- Emerging Issues in Offshoring
- Alignment of HIPAA and Part 2
- Use of Tracking Technologies
- Proposed Rule Overhauling the Security Rule

In the following pages, we take a deeper dive into each of these changes to highlight what you and your organization need to know to remain compliant.

Introduction to HIPAA

The Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health Act, and the regulations promulgated thereunder (collectively "HIPAA") is a federal privacy law which regulates use and disclosure of protected health information ("PHI"). PHI generally includes: (i) individually identifiable health information that is (ii) created or received by a provider or plan that (iii) relates to health care or payment for health care, which is (iv) maintained or transmitted in any form. Significantly, PHI is generally limited to information about health care or payment for health care, and does not ordinarily include employee information or commercially sensitive information such as trade secrets or intellectual property.

Notably, HIPAA only applies to: (i) "covered entities," which are healthcare providers that perform certain standard transactions electronically (*e.g.*, insurance eligibility transactions, submission of claims, etc.), health plans, and healthcare clearinghouses; and (ii) "business associates", which are persons or entities that perform certain functions or activities that involve use or disclosure of PHI on behalf of, or provide services to, a covered entity or an upstream business associate. It is important to note that although HIPAA only applies to certain regulated parties, state medical privacy laws remain an important consideration as they can apply to a broader range of situations.

HIPAA is comprised of three primary parts, including:

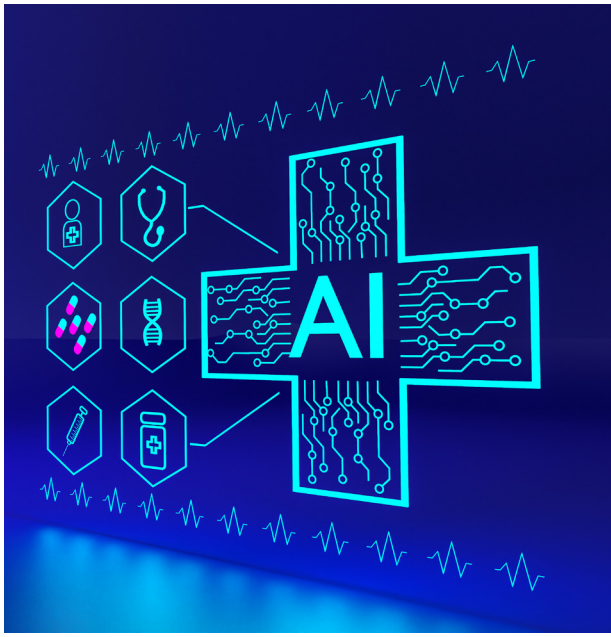
Privacy Rule - Regulates use and disclosure of PHI by regulated parties and requires implementation of certain measures, such as policies, procedures, and Notices of Privacy Practices, as well as execution of Business Associate Agreements, among others. *See* 45 § CFR 164.500 et seq.

Security Rule - Requires regulated parties to adopt administrative, technical, and physical safeguards to protect the security of electronic PHI (also known as "ePHI"). *See* 45 CFR § 164.300 et seq.

Breach Notification Rule - Requires regulated parties to notify individuals, certain agencies, and the media of breaches of unsecured PHI. *See* 45 CFR § 164.400 et seq.

Compliance with each of HIPAA's three parts is critical for regulated parties. Failure to comply with HIPAA may result in civil and criminal penalties, as well as significant costs associated with furnishing required notifications, credit monitoring, corrective action plans, and litigation expenses.

Privacy Challenges for Artificial Intelligence



Developments in artificial intelligence ("AI") are transforming day-to-day life, and the healthcare industry is no exception. AI's future in health care is bright with promise as we expect it to drive efficiencies in operations by supplementing professionals. Such supplementation can take different forms. For example, AI can be used to identify abnormalities or areas of concern in radiology reports, which a provider can then use as a reference. Similarly, AI also has tremendous potential in the remote monitoring space and in the healthcare space. Interestingly, AI can also work to address provider burnout by automating certain clerical and administrative tasks and allowing providers to focus on patient care.

Despite the promised benefits of AI, adoption and use of such technologies presents a number of compliance challenges. Chief among such challenges stands HIPAA and other privacy-related authorities. In particular, AI is data hungry. This is particularly true as AI is ordinarily trained on large pools of data to refine the AI to more closely mimic human behavior and decision making patterns. Organizations operating in the healthcare space will need to ensure that they have the appropriate rights and licenses to use data, including patient data, which is derived from third parties. Of particular interest, some AI tools may use the data they process to train the underlying AI technology, even without the user's awareness. It is imperative that parties review terms of use, privacy policies, and other contractual provisions carefully to assess how data may be used as well as to ensure that they have secured the appropriate consents.

Separately, healthcare organizations will need to ensure that any use of data in correlation with AI conforms to applicable privacy laws. This is critical, as such laws often prohibit commercialization of information or otherwise prohibit use of information for product development without patient consent, notice, or some measure of anonymization. In fact, parties leveraging the latest AI tools may not realize that the tools are using health information for training purposes, which may trail into commercialization.

Quick Compliance Tips

- Assess your organization's use of AI at both the enterprise and workforce member levels. Even if you do not expect that AI is being used, it likely is at the workforce member level!
- Consider whether vendors providing AI solutions are using your organization's data to improve their products.
- Adopt policies and procedures providing guidelines for responsible use of AI and which specifically address use of personal information.
- Organize a committee or other team to oversee adoption, use, and development of AI.

The State of Reproductive Healthcare Privacy

Since the *Dobbs v. Jackson Women's Health Organization* decision (which overturned the landmark *Roe v. Wade* decision), the healthcare industry has continued to grapple with renewed concerns over patient privacy and reproductive health care. Legislators and regulators have not been idle, establishing a patchwork of authorities which require careful navigation and consideration.

Federal Treatment of Reproductive Healthcare Privacy

In April of 2024, the Office of Civil Rights ("OCR") issued a Final Rule (the "Reproductive Final Rule") to expand HIPAA's protections around reproductive health privacy. Under the Reproductive Final Rule, the use or disclosure of PHI was prohibited where such use or disclosure was for the purpose of a criminal, civil, or administrative investigation into, or proceeding against, any person seeking, obtaining, providing, or facilitating lawful reproductive health care. Similarly, the Reproductive Final Rule also prohibited use or disclosure of PHI to impose criminal, civil, or administrative liability on any person for seeking, obtaining, providing, or facilitating reproductive health care.

The Reproductive Final Rule became the target of several lawsuits, including one filed by the Texas Attorney General as well as another filed by fifteen (15) State Attorneys General. The foregoing lawsuits centered on arguments that OCR exceeded the scope of its rulemaking authority in enacting the Reproductive Final Rule. Significantly, on June 18, 2025, the U.S. District Court for the North District of Texas issued an order vacating the Reproductive Final Rule, holding that "HHS lacked clear delegated authority to fashion special protections for medical information produced by politically favored medical procedures." *See* Purl v. U.S. Dep't of Health and Human Servs., et al., No. 2:24-cv-00228-Z (N.D. Tex. 2025). It is unclear whether the ruling will be appealed, but it is anticipated that the U.S. Department of Health and Human Services ("HHS") will likely not pursue further action.

State Treatment of Reproductive Healthcare Privacy

Several states have taken steps to protect healthcare providers, patients, and others involved in reproductive health care. Although state laws vary across jurisdictions, generally they limit (or outright prohibit) the disclosure of information related to reproductive health care that was lawfully received by a patient and furnished by a healthcare provider. For example:

- California amended its Confidentiality of Medical Information Act to prohibit disclosure of medical information related to an individual seeking or obtaining an abortion in response to a subpoena or even to law enforcement for purposes of enforcing a state's laws that interfere with the patient's rights under the Reproductive Privacy Act, among other prohibitions. Cal. Civ. Code § 56.108.
- In November 2024, New York voters approved Proposition One, which amended the New York State Constitution to explicitly protect against discrimination based on reproductive healthcare decisions and to recognize reproductive autonomy as a fundamental right in New York. Furthermore, certain New York clerks have refused to enforce out-of-state judgments penalizing providers for offering legal reproductive services by citing New York's Shield Law (a collection of statutes which are broadly intended to provide certain protections for providers and patients furnishing or receiving reproductive or gender affirming care).

With individual states adopting their own unique approaches to reproductive health privacy, regulated parties must now navigate a web of authorities in an already sensitive environment.

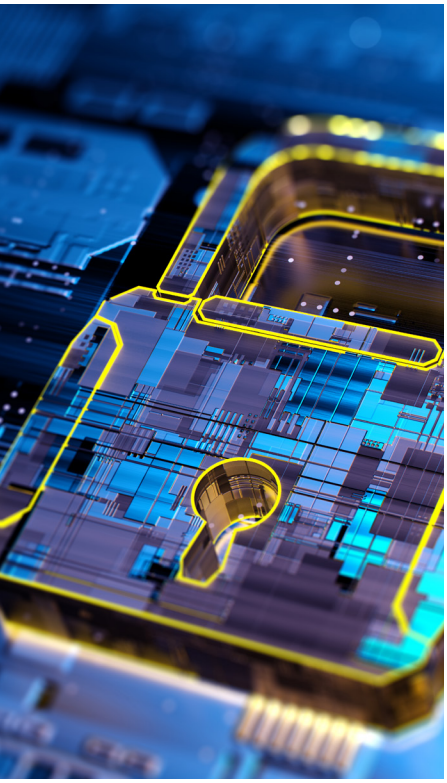
Conclusion

The world of reproductive healthcare privacy remains increasingly complex due to competing federal and state interests, a shifting political landscape, as well as evolving technologies and delivery methods. While the Reproductive Final Rule faces an uncertain future, state laws and consumer privacy regulations are filling the gap by creating an overlapping and sometimes conflicting patchwork of legal authorities. It is important for healthcare providers, insurers, and digital health platforms to ensure compliance with both federal requirements and state level regulations as well as taking proactive steps to have clear policies on data sharing and privacy audits, as well as engage in strategic communication with legal counsel.

Quick Compliance Tips

- Implement policies and procedures to address use and disclosure of reproductive healthcare information consistent with applicable authorities.
- Update your organization's Notice of Privacy Practices and privacy policy to assess use and disclosure of reproductive health information.

Recognizing Your Data as an Asset



Data has emerged as a valuable modern-day asset. While many industries have found data management to be a key factor in business revenue streams and strategy, the healthcare industry has generally hesitated to transition from a traditional data protection role to one that proactively maximizes the potential of data. This is especially true in the context of personally identifiable information and protected health information (collectively "PII"). In recognizing the value of data, Data Programs are intended to formally ensure that certain data, including PII, can be tapped as an asset as well as to operationalize steps to maximize its value in a manner consistent with applicable laws, contracts, and ethical standards. This presents unique opportunities and challenges, and can be a key factor in how an organization maintains a competitive edge and how the public regards its level of corporate citizenship.

There is no such thing as a one-size-fits-all Data Program. Organizations collect and receive different forms of data through unique arrangements and from varying sources, and each has customized operational goals and safeguards. In addition, different authorities may control, each of which will dictate how PII may be monetized. In particular, federal and state laws, internal policies, and third-party contracts govern what parties may permissibly do with PII. A good Data Program provides protective guardrails to avoid running afoul of applicable prohibitions related to selling, sharing, or using data. Within those guardrails, there are a number of mechanisms and venues where data may be used as a tangible asset, such as:

Data Sale - Configure data in a manner that allows for direct sale to third parties, resulting in a revenue stream of cash or other consideration (to support organizational initiatives/mission). For example, PII may need to be de-identified, including through the growing use of HIPAA Expert Determination methodology and the use of third parties to assist with the HIPAA Safe Harbor methodology. Notably, third-party vendors are often engaged to facilitate the processing component of reconfiguring PII for use.

Data Leasing and Licensing – Data sets can be leased for a fixed term or for a limited purpose with mandatory destruction/return. Such an approach allows an organization to retain full ownership and rights to data and ensures the dataset value does not depreciate due to copies maintained by a third party for perpetuity.

Data Derivative Rights - Secure data rights to deidentified, derived, and residual data where data could be enriched, reconfigured, or otherwise "cleaned" by third parties for purposes outside of an organization's enterprise. Due to the growth of AI and machine learning, algorithms and software built on derivative PII are becoming commonplace and, in some cases, valuable. A Data Program may contemplate how to ensure an organization maintains a stake in any profitable by-product generated by any part of data sourced by the organization.

Data as Equity - Contribute data assets as a substitute for traditional capital when investing in an organization or another initiative. For example, an organization may contribute data in exchange for an equitable stake in an emerging-growth organization or product. Thereafter, the stake can be sold to investors or other third parties. In this scenario, data serves as a substitute for traditional capital to secure an investment.

Data as Capitalization and Partnership Incentive - Many organizations seeking to invest or to acquire assets of an organization will be keenly interested in the availability of data. Specifically, the organization in question may have an independent use for the data and as such, data can be treated as an economic or strategic asset for investment purposes. In addition, the availability of, and promise of access to, data can entice potential partners to join in economic ventures or other initiatives.

Data as Leverage - Data can offer a competitive advantage or can prove valuable to an acquiring party. Recognize the potential value of the data involved in any arrangement and leverage that access and use to maximize benefits, including competitive service fees, extended term limits, or mutual data access and use.

Quick Compliance Tips

- Assess the data which your organization generates or otherwise receives to determine whether data is available to be leveraged.
- Assess whether leveraging data for your organization's internal operations or externals offerings is consistent with its business objectives or could provide a valuable economic opportunity.

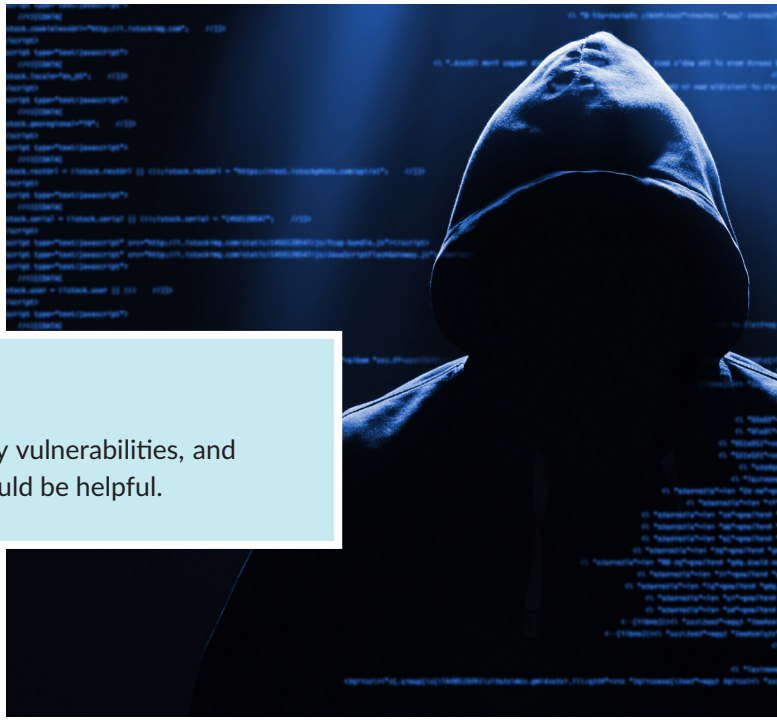
Health Care Needs More Hackers?

Our daily newsfeeds are peppered with reports of new and emerging cyberattacks which compromise highly sensitive information, such as personal or health information. Such attacks are significant not only due to the nature of the information at issue, but also due to the fact that responding to cyberattacks, related litigation, and government investigations often come with hefty price tags. Ethical hacking (also referred to as "white-hat hacking" or "good faith hacking") presents a potential solution to mitigate cyberattacks.

Ethical hacking is a practice through which a party intentionally and proactively probes computer systems, networks, or applications for security vulnerabilities. The goal is generally to identify and remediate vulnerabilities before they can be exploited. Ethical hacking comes in a variety of forms, such as through formal engagement of vendors to facilitate penetration testing as well as through programs which offer financial rewards to private parties who report vulnerabilities. In effect, hackers can be leveraged to promote security rather than to exploit vulnerabilities. Notably, many of the largest technology companies and social media organizations have implemented ethical hacking programs, often referred to as "bug bounty programs." These programs often make good business sense, as average payouts for identified vulnerabilities ordinarily pale in comparison to the average cost of breaches, which can quickly rise into the millions of dollars.

It is critical that regulated parties take steps to ensure compliance with HIPAA, such as by ensuring that allowing ethical hackers to access PHI is conducted for a permissible purpose, executing business associate agreements with formally engaged parties that qualify as business associates, and work to limit PHI implicated to the minimum amount necessary, among other measures. Failure to ensure that an ethical hacking program is conducted in compliance with HIPAA could result in significant civil penalties.

It is critical that parties take cybersecurity seriously. Ethical hacking presents a tremendous opportunity to identify and address vulnerabilities before they can be exploited to detrimental effect. Thoughtful consideration of the legal hurdles discussed above is critical to ensure that ethical hacking is conducted in a compliant and effective fashion.



Quick Compliance Tips

- Assess your organization's practices for identifying security vulnerabilities, and determine whether proactive engagement of third party could be helpful.

Alignment of HIPAA and Part 2

In February of 2024, HHS and the Substance Abuse and Mental Health Services Administration ("SAMHSA") released the long anticipated Final Rule (the "Part 2 Final Rule") to revise the Confidentiality of Substance Use Disorder ("SUD") Patient Records regulations at 42 C.F.R. Part 2 ("Part 2"). In particular, Part 2 protects SUD records created by federally assisted programs. These confidentiality protections were initially enacted to help address concerns around the use of SUD information in criminal proceedings, employment and housing discriminatory practices, child custody hearings, and other administrative matters.

Providers subject to Part 2 are generally prohibited from disclosing any information that would identify a person as having or having had a SUD without the person's consent. Because Part 2 regulations were implemented in 1975, over two decades before the implementation of HIPAA, providers have historically struggled to comply with both HIPAA and Part 2. Specifically, providers subject to HIPAA were also required to comply with Part 2 for SUD records, which forced those providers to comply with often inconsistent standards for different types of health information. Naturally, the presence of two competing standards caused confusion, increased administrative burdens, and often obstructed provider access to patient information. The Part 2 Final Rule includes several changes to align Part 2 more closely with HIPAA and to reduce those administrative burdens, as summarized below:

Patient Consent. Patients can now provide a single consent to authorize all future uses and disclosures related to treatment, payment, or healthcare operations ("TPO"), instead of requiring a new consent for each disclosure. A consent will generally remain effective unless it is revoked by the patient.

Enhanced Protections for Counseling Session Notes. Parallel to HIPAA protections for psychotherapists' notes, clinicians' notes from SUD counseling sessions must be maintained separately from other patient records and require specific patient consent to disclose. Thus, if a patient provides a general TPO consent, the counseling session notes will fall outside the scope of that consent and will not be disclosed.

Breach Notification. Breaches of Part 2 records will be subject to the same patient notification requirements of the HIPAA Breach Notification Rule.

Penalties. Violations of Part 2 will now be subject to the same civil and criminal enforcement authorities that apply to HIPAA violations.

Patient Complaints. In addition to or in lieu of filing a complaint for an alleged violation under the Part 2 program, patients can choose to file a complaint directly with HHS. Further, patients can request a list of all disclosures made with consent for the past 3 years.

Public Health Authority Disclosure. De-identified records may generally be disclosed to public health authorities without patient consent, in accordance with the HIPAA Privacy Rule.

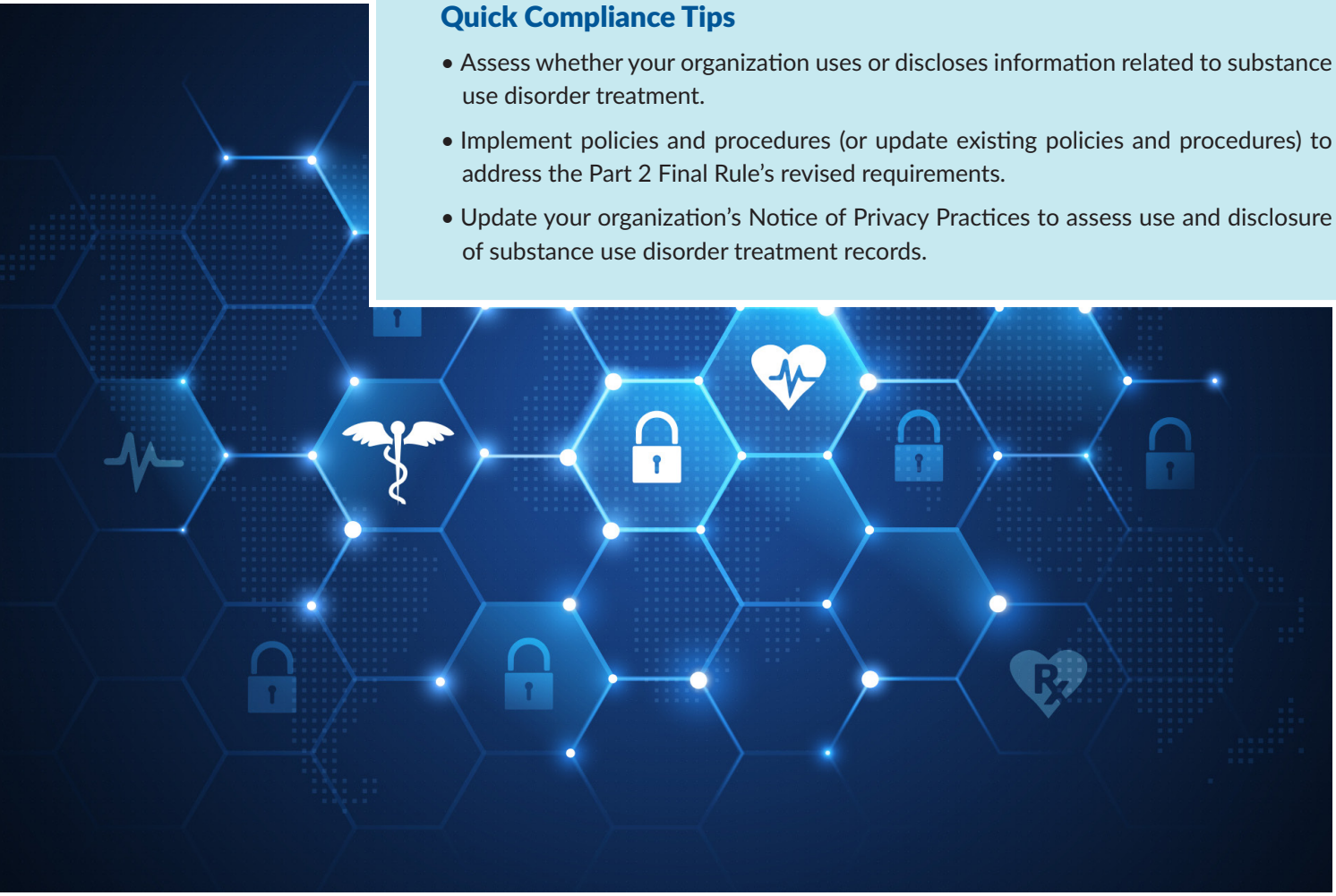
Investigations Safe Harbor. Individuals working for investigative agencies that unlawfully obtain a confidential Part 2 record without the requisite court order will have limited civil and criminal liability, so long as the individual acted with "reasonable diligence" in evaluating whether the provider is subject to Part 2 prior to making the record request.

Flexibility on Redisclosures. HIPAA regulated parties may redisclose SUD records received pursuant to a TPO authorization in a manner consistent with the HIPAA Privacy Rule, reducing the need for segregating or segmenting SUD records from other PHI in daily operations.

The Part 2 Final Rule took effect on April 16, 2024 and entities are obligated to ensure compliance by February 16, 2026. For more information on the Part 2 Final Rule, see the HHS Final Rule Fact Sheet.

Quick Compliance Tips

- Assess whether your organization uses or discloses information related to substance use disorder treatment.
- Implement policies and procedures (or update existing policies and procedures) to address the Part 2 Final Rule's revised requirements.
- Update your organization's Notice of Privacy Practices to assess use and disclosure of substance use disorder treatment records.



Use of Tracking Technologies

In December of 2022, OCR published guidance (which was updated in early 2024) (the "Guidance") indicating that the use of third-party tracking technologies (*e.g.*, cookies, web beacons or tracking pixels, session replay scripts, fingerprinting scripts, etc.) may result in a regulated party's disclosure of PHI to such third parties depending on the location of the tracking technology and the information collected. In particular, the Guidance indicated that an impermissible disclosure of PHI may occur not only on webpages where the user patient had authenticated himself/herself (such as by logging into a portal or providing other identifying information), but also on unauthenticated webpages where tracking technologies collected IP addresses which could be traceable to the user patient. Since 2022, we have observed a sharp increase in class action lawsuits and regulatory enforcement actions which specifically targeted use of third-party tracking technologies on healthcare organization websites. In recognition of the increased exposure to hospitals and other providers, the American Hospital Association (the "AHA") (along with other parties) filed an action arguing that issuance of the Guidance exceeded HHS's statutory authority under HIPAA and imposed unreasonable compliance burdens.

In June of 2024, the U.S. District Court for the Northern District of Texas issued an opinion vacating HHS's guidance on the use of third-party tracking technologies under HIPAA. The court rejected HHS's broad interpretation of PHI to include a user's IP address when the user visits a public facing, unauthenticated webpage with information about specific health conditions or healthcare providers ("Proscribed Combination"). It found that the Guidance unlawfully expanded the definition of PHI to include data that could not reasonably identify an individual or their health condition without knowing the user's subjective intent for the visit. The court determined that this expansion was not supported by HIPAA's statutory language and exceeded the bounds of HHS's regulatory authority.

Granting partial summary judgment to the plaintiffs (including the AHA), the court declared the Proscribed Combination unlawful and ordered its vacatur. This means the Guidance related to the Proscribed Combination cannot be enforced and must be removed from the Guidance. Despite this, the Guidance which is related to the authenticated portion of a regulated party's website still stands, and regulated parties should still ensure that any use of tracking technologies on authenticated webpages complies with HIPAA. In particular, the following material points of the Guidance remain pertinent:

- Regulated parties must configure any user-authenticated webpages that include tracking technologies to allow such technologies to **only** use and disclose PHI in compliance with the HIPAA Privacy Rule and must ensure that ePHI collected through the website is protected and secured in accordance with the Security Rule.
- Regulated parties must ensure that disclosures of PHI to tracking technology vendors is permissible under the Privacy Rule.
- Regulated parties must ensure that they have executed Business Associate Agreements with tracking technology vendors.
- Regulated parties must consider use of tracking technologies in their periodic security risk analyses, as prescribed by the Security Rule.

Accordingly, HIPAA-regulated parties should continue to investigate and analyze their use of tracking technologies. In fact, questions about tracking technology use are becoming common place in diligence and increasingly frequent in seller representations and warranties. Further, the use of tracking technologies can easily be gleaned by plaintiffs' counsel, regulators, and other interested parties.

Quick Compliance Tips

- Assess your organization's websites to identify use of cookies, pixels, and other tracking technologies.
- Ensure your organization has implemented a Business Associate Agreement with a vendor providing or hosting a tracking technology.
- Ensure your organization considers use of third-party tracking technologies in its security assessments.
- Ensure your organization's public-facing privacy policies clearly addresses use of third-party tracking technologies.

Emerging Issues in Offshoring

Participants in the healthcare space are increasingly relying on offshore vendors and resources to operate, such as for claims processing, call center staffing, and technical support. Such arrangements are often appealing as offshore contractors frequently provide cost savings and other efficiencies that may be critical to offerings and pricing models. Opponents of offshoring ordinarily cite increased security vulnerabilities in foreign networks as a real risk, particularly as offshore services frequently involve access to large amounts of health information. It is vital that the parties considering an offshore arrangement carefully navigate the interplay of laws, regulations, and guidance, which are complex and often inconsistent, to ensure compliance.

HIPAA -HIPAA and its implementing regulations are a centerpiece of healthcare privacy discussions. Interestingly, HIPAA does not explicitly prohibit offshoring of patient data, but does require that regulated parties implement reasonable and appropriate administrative, physical, and technical safeguards to ensure the privacy and security of protected health information and that business associate agreements are executed where appropriate, among a number of other compliance measures. As a result, regulated parties must take steps to ensure compliance with HIPAA, particularly when using offshore resources which may present unique privacy and security considerations.

Medicare Authorities -The Centers for Medicare and Medicaid Services ("CMS") issued guidance to Medicare Advantage organizations and prescription drug plan sponsors requiring execution of "extraordinary measures" to ensure that offshore relationships appropriately safeguard patient data. In particular, the guidance requires completion of attestation which must address: (1) the identity and function of the offshore subcontractor; (2) a description of any protected health information that will be accessible by the offshore subcontractor; and (3) the safeguards adopted by the offshore subcontractor to safeguard protected health information. In addition to the attestation, the regulated parties must take steps to audit the offshore subcontractor. It is important to note that the guidance does not prohibit offshoring of patient data, but it imposes a number of hurdles to such arrangements.

Medicaid Authorities – Although the Affordable Care Act prohibits states from making payments for items or services provided under a state plan (or a corresponding waiver) to a financial institution or entity located outside of the United States, CMS clarified that tasks that support administration of the plan, which may require payments to parties located outside of the United States, may be permitted. In light of this clarification, payments exclusively for administrative functions are permitted for financial institutions or entities located outside of the United States. Building on the foundation established by federal law, it is important to consider state laws and regulations specific to Medicaid, as offshoring limitations vary across jurisdictions and are often addressed in frequently-revised manuals. For example, Texas authorities prohibit managed care organizations and their subcontractors from allowing certain confidential information they receive on behalf of the Texas Health and Human Services Commission (the "Commission") to be moved outside of the United States by any means. In addition, managed care organizations and their subcontractors are prohibited from permitting remote access to the Commission's information, systems, or deliverables from a location outside of the United States. It is important to examine Medicaid-specific authorities adopted by the pertinent states to determine whether they impose independent limitations or requirements on use of offshore resources.

State Authorities -Beyond Medicaid-specific authorities, a number of states have taken steps to limit or otherwise outright prohibit offshoring of patient data. For example, the Florida Legislature amended the Florida Electronic Health Records Exchange Act in 2023 to prohibit certain healthcare providers from storing qualified electronic health records outside of the United States, its territories, or Canada. Similarly, some governors have issued executive orders prohibiting offshoring of certain activities which are paid for by state agencies, such as in Ohio, which prohibit state agencies from entering into any contract which uses any funds within such agency's control to purchase services outside of the United States.

Contractual Authorities -Contracts with payors, Medicare Advantage organizations, state Medicaid agencies, and a broad array of other parties may also incorporate restrictions or requirements associated with offshoring. This is significant as contracts may limit or prohibit offshoring even where federal or state laws and regulations would not prohibit it. As a result, it is a best practice that healthcare organizations review their agreements to assess whether there are any specific contractual requirements or limitations associated with offshoring.

Looking ahead, parties with existing offshore arrangements, or who may be considering offshore arrangements, must carefully consider the many hurdles discussed above to ensure compliant operations.

Quick Compliance Tips

- Assess whether your organization currently, or may in the near future, engage with vendors based outside of the United States.
- Assess whether offshore vendors are able to store personal information or to create local copies of personal information (e.g., screenshotting, print, or downloading) outside of the United States.
- Assess upstream contractual limitations on use of offshore vendors or personnel, such as with respect to customers, payor, or other parties.

Proposed Rule Overhauling the Security Rule

HHS issued a Notice of Proposed Rule Making (the "Proposed Security Rule") on December 27, 2024 to significantly amend HIPAA's Security Rule, which sets forth the security standards for safeguarding ePHI by covered entities and their business associates. The Proposed Security Rule was expected, particularly in light of the significant increase in data breaches impacting the healthcare industry and the rise of large scale foreign cyberattacks. If finalized, it would overhaul HIPAA's Security Rule such that HIPAA-regulated parties would have significant work to complete as the Proposed Security Rule takes aim at several key areas of the Security Rule, the most significant of which we address below.

Standards for Assessing Adequacy of Safeguards

The Security Rule requires that covered entities and business associates implement reasonable and appropriate administrative, physical, and technical safeguards to protect the privacy and security of ePHI. As a starting point, and perhaps most significantly, the Proposed Security Rule removes the distinction between "required" and "addressable" safeguards, which has the ultimate effect of rendering all safeguard specifications to be required, subject to certain exceptions. This is significant as many regulated parties have historically construed the Security Rule's flexibility with respect to addressable safeguards (*i.e.*, which considered size, complexity, technical infrastructure, and resources in assessing the adequacy of safeguards) as a basis for neglecting or otherwise ignoring the addressable safeguards. The Proposed Security Rule would eliminate this distinction by requiring that regulated parties implement all of the standards and specifications but would continue to afford regulated parties with a measure of flexibility in how they go about satisfying the standards and specifications.

The Proposed Security Rule would not eliminate the Security Rule's flexible nature, but would expand the factors to be considered in assessing the adequacy of safeguards, which must now include:

1. The size, complexity, and capabilities of the regulated party;
2. The regulated party's technical infrastructure, hardware, and software security capabilities;
3. The costs of the security measures;
4. The probability and criticality of potential risks to ePHI; and
5. The effectiveness of the security measure in supporting the resiliency of the regulated party.

If implemented, regulated parties would be required to reevaluate their security practices to ensure that they have addressed all safeguards in an adequate manner. Critically, regulated parties will be on notice that safeguards which were previously considered "addressable" cannot be brushed away and must be implemented in an effective manner to ensure compliance with HIPAA.

Updated Safeguard Specifications

The Security Rule is perhaps best known for establishing a lengthy list of safeguards for how regulated parties should go about safeguarding ePHI. The Proposed Security Rule overhauls these requirements by adding a range of new safeguards, as well as by significantly expanding existing safeguards.

Written Inventory of Technology Assets and Network Map – The Proposed Security Rule requires development of a written inventory of technology assets, as well as a network map, in relation to which ePHI may be created, received, maintained, or transmitted. In addition, regulated parties must update the inventory and map on an ongoing basis, but at least once every twelve months or following a change in the regulated party's environment or operations that may affect ePHI. Development of the inventory and map will likely require a measure of technical expertise that many regulated parties may not maintain in-house, and will result in both administrative and cost burdens in terms of maintenance.

Encryption – The Proposed Security Rule clarifies that regulated parties must encrypt ePHI both in transit and at rest, while also providing a number of exceptions, such as where the technology assets currently in use do not support encryption and the regulated party establishes a written plan to migrate ePHI to a technology asset which does in fact support encryption. While not new, many regulated parties may not have appreciated the importance of ensuring encryption of ePHI when it is being transmitted, but also when it is being stored, such as on a local device, server, or even on a cloud. It will be vital for regulated parties to assess whether existing storage locations satisfy the encryption requirement. Similarly, it will be critical for regulated parties to assess whether they are transmitting ePHI in a manner which is not encrypted, such as through text messaging, e-mail, or other messaging applications.

Multi-Factor Authentication – The Proposed Security Rule requires regulated parties to deploy multi-factor authentication for any action that would change a user's privileges to the regulated party's relevant electronic information systems in a manner that would alter the user's ability to affect the confidentiality, integrity, or availability of ePHI, subject to certain exceptions. Regulated parties would be required to test the effectiveness of such technical controls at least once every twelve months or following an environmental or operational change.

Contingency Plans – The Proposed Security Rule expands the existing obligation that regulated parties implement written contingency plans, which must include policies and procedures for responding to emergencies such as fires, system failures, and natural disasters, among other occurrences. In particular, the Proposed Security Rule requires that regulated parties conduct and document the relative criticality of its relevant electronic information systems and technology assets, as well as that regulated parties implement written policies and procedures to restore loss of critical relevant electronic information systems and data within seventy-two hours of loss. Regulated parties would also be required to test such plans at least once every twelve months, document the results of such tests, and modify plans as reasonable and appropriate.

Network Segmentation – The Proposed Security Rule requires regulated parties to implement written policies and procedures that segment networks in a manner which limits access to ePHI through authorized workstations. In addition, the Proposed Security Rule requires implementation of technical controls to facilitate network segmentation. This requirement would obligate regulated parties to assess the technical setup of their respective networks, which would likely require consultation with technical experts.

Vulnerability Scans – The Proposed Security Rule would require regulated parties to conduct automated vulnerability scans to identify technical vulnerabilities in accordance with the regulated party's security risk analyses or at least once every six months, whichever is more frequent.

Penetration Testing – The Proposed Security Rule would require regulated parties to complete penetration testing in accordance with the regulated party's security risk analyses or at least once every six months, whichever is more frequent. Penetration testing would need to be conducted through a qualified person with appropriate knowledge of and experience with generally acceptable cybersecurity principles and methods.

Backups – The Proposed Security Rule would require regulated parties to deploy technical controls to create and maintain retrievable copies of ePHI which are sufficient to ensure that retrievable copies are no more than forty-eight hours old. In addition, the Proposed Security Rule requires deployment of technical controls that alert workforce members in real time of failures and error conditions in required data backups, as well as which record the success, failure, and error conditions of backups. The foregoing technical controls must be tested at least monthly.

While some regulated parties may have already implemented variations of the safeguards noted above, many have not. If finalized, the above technical safeguards would impose a significant administrative burden and cost on all regulated parties, many of whom may struggle to comply.

Updated Standards for Business Associate Agreements

The Proposed Security Rule makes a number of revisions to the requirements applicable to arrangements with business associates, including: (1) requiring business associates to notify covered entities upon activation of their contingency plans no later than twenty-four hours after activation (which would be required to be prepared under the Proposed Security Rule); and (2) requiring that covered entities obtain written verification from their business associates, at least once every twelve months, that such business associates have deployed technical safeguards required by the Security Rule.

If finalized, the proposed updates would require regulated parties to revisit their business associate agreements with existing vendors which would necessitate new negotiations and revisions to existing templates (if any) across enterprises. In addition, ensuring completion of the annual written verification would also present an administrative hurdle which would be difficult to track, particularly for business associates supporting many covered entities or covered entities relying on a broad array of business associates to sustain their operations.

Conclusion

It is important to note that the current Security Rule remains in effect until HHS publishes a Final Rule. A window for submission of public comments is currently underway, with a slated cut-off date of March 7, 2025. We anticipate that HHS will receive many comments to work through given the potential impact of the Proposed Security Rule. Opponents are particularly concerned about the costs associated with implementing and maintaining the required safeguards. In particular, some have contended that the Biden Administration's initial estimation was far too low, which predicted that that implementation costs would be $9 billion the first year with an additional $6 billion being expended across years two through five, with implementation costs threatening to raise the cost of healthcare services. See, e.g., College of Health Information Management Executives Letter, dated February 17, 2025. Due to the change in administration, the Proposed Security Rule will likely receive increased scrutiny and, therefore, it may be some time before a Final Rule is published. However, given the importance of mitigating cybersecurity risks in the healthcare industry, we expect the Proposed Security Rule will be finalized in some form. It will be vital to continue monitoring these developments.

Quick Compliance Tips

- While no immediate action is required, it may be helpful for your organization to monitor the notice and comment process to assess how HHS may ultimately resolve the rulemaking process.
- Consider assessing your organization's current security infrastructure and practices to analyze its alignment with HHS's stated priorities.

SheppardMullin

Hot Topics in HIPAA

2025