Protecting Patient Information

The Division of Consumer Affairs provides health care practitioners with this alert to support practitioners in protecting both their patients and themselves with respect to data security and disclosure of patient information. In the wake of the Supreme Court's decision in *Dobbs v. Jackson Women's Health Organization*, it is more crucial than ever that health care practitioners take measures to secure patient data and information.

Data Minimization

The best way to prevent a data breach is to avoid collecting unnecessary data in the first place. "Data minimization" means collecting and retaining only the information necessary to treat patients.

Adopting smart practices for maintaining a website is crucial to data minimization. Many practitioners may not be aware that their websites are configured to collect, track, and analyze user data. For example, the website may collect a user's IP address (a proxy for location) and information about other websites the user has visited. A website may also share user-inputted information with third parties, including the user's name, phone number, email and home addresses; the healthcare service that the user is seeking; and a description of the user's health issue. Many practitioners may not even be aware that their websites are sharing such information with third parties.

There is a simple fix for this problem: practitioners can simply not install on their websites the tracking, analytics, and marketing tools that automatically collect and share user data with third parties. A practitioner can also use an independent cybersecurity service to audit an existing website for privacy and security vulnerabilities.

Reasonable Security Controls

Even if practitioners minimize the data that they collect, they will still possess protected health information ("PHI"). Below are some practical steps to help practitioners protect PHI and other identifying information:[1]

- Require patient and employee passwords to include special characters and numbers, and require multi-factor authentication;
- Install and enable a firewall, intrusion detection/prevention systems, and other security solutions;
- Keep all security software up to date;
- Encrypt stored PHI and other sensitive information, including but not limited to account information, biometric identifiers, device identifiers, home addresses, email addresses, financial information, government identification, health insurance information, IP addresses, medical record numbers, names, passwords, phone numbers, and Social Security Numbers;
- Use end-to-end encryption to send and receive PHI electronically;
- Develop data retention policies that cut down on the unnecessary retention of data and cull files to minimize the amount of sensitive data that is stored, consistent with the federal Health Insurance Portability and Accountability Act ("HIPAA") and New Jersey law;
- When deleting PHI, do so securely (such as with specialized software);
- Securely delete PHI before discarding or reusing computers or digital devices;
- Maintain physical control of computers and digital devices, such as with locked doors;
- Use access controls to provide employees with only the minimum system rights necessary to do their jobs; and
- Train all employees in digital safety (such as how to recognize phishing attempts and other red flags) to prevent data breaches.

continued

Disclosure of Patient Information

Licensed health care providers have a long-standing legal and ethical duty of confidentiality to their patients. Licensees may not release patient records without the patient's consent, except in limited circumstances.

On June 29, 2022, the federal Department of Health and Human Services ("HHS") issued guidance entitled "HIPAA Privacy Rule and Disclosures of Information Relating to Reproductive Health Care." The HHS guidance explains that HIPAA permits covered entities to disclose PHI in limited instances, such as when disclosure is required by law or sought for law enforcement purposes through legal process (such as a subpoena or court order).[2] So while HIPAA does not *require* covered entities to make disclosures, it permits covered entities to comply with other laws that require practitioners to disclose PHI. Practitioners should consult with counsel regarding their obligations under HIPAA and other applicable laws.

The HHS guidance emphasizes that HIPAA's grant of permission to disclose PHI "as 'required by law' is limited to 'a mandate contained in law that compels an entity to make a use or disclosure of PHI and that is enforceable in a court of law.'"[3] For example, HIPAA permits a covered entity to comply with a valid, enforceable subpoena or court order. The HHS guidance also explains that HIPAA does not permit disclosures—to law enforcement or otherwise—that are not legally required or that exceed what is legally required. In order for a request from law enforcement to fall within the HIPAA "required by law" exception, the request must be enforceable in a court of law. Voluntary disclosures to law enforcement do *not* fall within this HIPAA exception.

In addition, on July 1, 2022, Governor Murphy signed into law P.L. 2022, c. 51 ("Chapter 51"). Chapter 51 prohibits a HIPAA covered entity from disclosing any communication from a patient or information obtained from the personal examination of a patient relating to reproductive health care services that are permitted under New Jersey law, unless the patient or that patient's conservator, guardian, or other authorized legal representative explicitly consents in writing. A covered entity must inform the patient of the right to withhold written consent at or before the time reproductive health services are rendered or at the time the patient discloses information relating to reproductive health services previously rendered.[4]

* * *

In the aftermath of the Supreme Court's decision in *Dobbs v. Jackson Women's Health Organization*, it is more important than ever that health care practitioners take action to safeguard patient data and information. Adopting the measures outlined above is a crucial step. Practitioners should regularly review their data security practices and consult with counsel to ensure that they are fulfilling their obligations to protect patient data and information.

Resources:

HIPAA Privacy Rule and Disclosures of Information Relating to Reproductive Health Care

HIPAA for Professionals

Security Rule Guidance Material

Cyber Security Guidance Material

Training Materials

Health Information Technology

How may the HIPAA Privacy Rule's minimum necessary standard apply to electronic health information exchange through a networked environment?

---

[1] This list is not comprehensive and is meant only to inform practitioners of practical steps they can take to safeguard data. It does not constitute legal advice or a description of practitioners' legal obligations.

[2] A "covered entity" means a "health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter[,]" a health plan, and a health care clearinghouse. 45 C.F.R. § 160.103. Thus, "[e]very health care provider, regardless of size, who electronically transmits health information in connection with certain transactions, is a covered entity. These transactions include claims, benefit eligibility inquiries, referral authorization requests, or other transactions for which HHS has established standards under the HIPAA Transactions Rule." https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

[3] See 45 C.F.R. § 164.103 (definition of "Required by law").

[4] Chapter 51 provides that written consent is not needed to disclose information pursuant to New Jersey law or the Rules of Court, to the covered entity's attorney or insurer in defense of a claim against the covered entity, to certain New Jersey State agencies, or in cases of suspected child abuse. N.J.S.A. 2A:84A-22.18(b)(1)-(3). Chapter 51 explicitly states that the provision of or material support for reproductive health care services that are permitted under New Jersey law does not constitute child abuse. N.J.S.A. 2A:84A-22.18(b)(4).