Challenges Facing Communication About HIPAA And Possible Solutions

Posted on January 9, 2020

Introduction

Securing patients' protection and the privacy of their health data is an imperative moral and legal prerequisite for players and practitioners in the healthcare industry. Various legal provisions protect individual privacy and offer guidelines to hospitals and other involved organizations. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal statute enacted by the U.S. Congress that provides a legal framework for safeguarding protected health information held by covered entities and their business associates. Other than confidentiality and privacy, HIPAA also seeks to improve health insurance portability, reduce healthcare fraud and abuse, and establish administrative standards for electronic healthcare transactions. The Privacy, Security, and Breach Notification Rules have contributed to a national framework for protecting health information, but HIPAA does not apply to every organization or every health-related technology (Office of the National Coordinator for Health Information Technology [ONC], 2026). Notwithstanding such protections, the rules can be difficult to communicate in areas such as minors, personal representatives, state-law interaction, emergency disclosures, cybersecurity, and consumer health applications. In the face of such issues, communication about HIPAA presents serious challenges to players and stakeholders in the healthcare industry that need to be examined more closely and solutions developed. This paper examines current problems facing attempts to communicate HIPAA rules to stakeholders and proposes possible solutions.

Challenges Facing HIPAA Rules

The Department of Health and Human Services (HHS), which enforces the HIPAA Privacy and Security Rules at the federal level, faces critical challenges in explaining how the rules apply where minors are involved. Healthcare practitioners, insurance companies, hospitals, minors, and parents have expressed uncertainty about how much control parents and guardians have over a minor's protected health information. HIPAA does not itself establish one universal age at which every person becomes an adult. Instead, state or other applicable law generally determines the age of majority, whether a minor can consent to particular healthcare services, and whether a parent is the child's personal representative. As a general rule, a parent or legal guardian with authority to make healthcare decisions for an unemancipated minor is treated as the minor's personal representative. Exceptions may apply when the minor lawfully consents to a service, another person is authorized to consent, a parent agrees to a confidential relationship, or the provider reasonably believes that treating the

parent as the personal representative could endanger the child (U.S. Department of Health and Human Services [HHS], 2023).

The rules may apply differently in various medical scenarios with different implications. One of the most challenging areas relates to substance-use treatment, contraception, sexual health, mental health, and other services for which state law may allow a minor to consent independently. In these situations, the parent may not be the personal representative for the information connected with that particular treatment. This does not mean that HIPAA generally excludes parents from their children's care, nor does it mean that minors always control all medical records. Rather, providers must assess the specific service, state law, consent arrangement, professional judgment, and any safety concerns. Communicating these distinctions is difficult because a simple statement such as "parents always have access" or "minors always have privacy" is legally inaccurate (HHS, 2023).

Closely related to the above is compliance with state laws versus HIPAA. HIPAA generally establishes a federal floor of privacy protection. A contrary state law may be pre-empted, but an exception applies when the state provision relates to the privacy of individually identifiable health information and is more stringent than the HIPAA requirement. The term "more stringent" has a regulatory definition, but applying it may still require legal and compliance analysis. Consequently, providers should not assume that HIPAA automatically overrides every state privacy law or that state law automatically replaces HIPAA. Organizations may need to comply with both frameworks and document which rule controls the particular issue (Legal Information Institute, 2026).

Another critical issue is the application of HIPAA in the face of public-safety concerns or emergencies. In some cases, a patient's health information may be relevant to preventing or reducing a serious and imminent threat, coordinating care, notifying family members, or responding to an emergency. HIPAA is not a blanket code of silence. The Privacy Rule contains permissions for treatment, healthcare operations, disclosures to personal representatives, certain disclosures to family and others involved in care, public-health activities, law-enforcement situations, and efforts to avert a serious threat to health or safety. However, the conditions and minimum-necessary requirements differ by circumstance. Fear of penalties, incomplete training, or overly restrictive institutional policies may cause staff to withhold information that HIPAA would permit them to share. Conversely, casual or excessive disclosure may violate privacy. The communication challenge is therefore to teach staff when sharing is permitted, when authorization is required, and how to disclose only the information reasonably necessary.

Electronic communication creates an additional challenge. Smartphones, text messages, patient portals, cloud systems, and mobile devices can make communication faster but also create risks involving unauthorized access, lost devices, weak authentication, insecure transmission, and incomplete records. HIPAA does not ban electronic communication or texting. The Centers for Medicare & Medicaid Services states that hospitals and critical access hospitals may text patient information and orders when they use a HIPAA-compliant secure texting platform and meet applicable record, security, and authentication requirements (Centers for Medicare & Medicaid Services [CMS],

2024). Ordinary consumer messaging applications, personal accounts, or unapproved devices may not provide the safeguards, access controls, auditability, and retention required by organizational policy.

Cybersecurity is another growing communication problem. Covered entities and business associates must protect the confidentiality, integrity, and availability of electronic protected health information. Yet employees may misunderstand the Security Rule as a purely technical responsibility assigned to the information-technology department. In reality, administrative, physical, and technical safeguards involve leadership, workforce training, risk analysis, access management, incident response, contingency planning, device controls, and technical security measures. NIST's updated HIPAA Security Rule guide maps regulatory requirements to modern cybersecurity practices and helps organizations translate legal standards into operational controls (National Institute of Standards and Technology [NIST], 2024).

In the modern age of mobile technology, health applications create a separate but related problem. HIPAA protects health information when it is maintained or transmitted by a covered healthcare provider, health plan, clearinghouse, or business associate. It generally does not apply merely because information is health-related. When consumers voluntarily enter information into an app or service that is not acting for a HIPAA-covered entity, the data may fall outside HIPAA. The Federal Trade Commission's revised Health Breach Notification Rule clarifies its application to many health apps, connected devices, and similar technologies that are not covered by HIPAA (Federal Trade Commission [FTC], 2024). A 2024 systematic review found that patients consistently expressed concerns about privacy, confidentiality, security, transparency, and awareness when using mHealth applications (Alhammad et al., 2024). Therefore, telling consumers that an app is "HIPAA compliant" may be incomplete or misleading unless the organization explains the app's role, data flows, third-party sharing, and applicable laws.

Proposed Solutions

Regarding the application of HIPAA alongside state law, a practical solution is the provision of clear, scenario-based guidance. Organizations should develop decision trees for minors, personal representatives, confidential services, state-law exceptions, requests from family members, public-safety disclosures, and access to records. The phrase "more stringent" should be explained through examples relevant to the organization's state and services. Privacy officers and legal counsel should maintain current state-law matrices rather than asking front-line staff to resolve pre-emption questions independently. Communication materials should emphasize that HIPAA is usually a federal floor, not the only privacy rule (Legal Information Institute, 2026).

On the question of sharing information for care or public-safety purposes, organizations should replace a culture of automatic refusal with trained professional judgment. Staff should know that HIPAA permits many routine treatment disclosures and contains specific permissions for emergencies

and serious threats. Training should distinguish what is legally permitted from what an institution chooses as a stricter policy. It should also teach documentation, identity verification, minimum-necessary principles where applicable, and escalation to a privacy officer when facts are uncertain. This approach can reduce both inappropriate silence and inappropriate disclosure.

Communication about minors should be designed for three audiences: healthcare workers, parents, and adolescents. Consent forms and privacy notices should explain when parents normally have access, when state law allows confidential care, how portal access may change, and how safety exceptions work. Providers should avoid absolute promises of confidentiality before reviewing the law and the clinical circumstances. They should also tell adolescents when information may need to be shared to protect them or someone else. HHS guidance should be incorporated into organization-specific protocols rather than left as a legal document that staff rarely consult (HHS, 2023).

Healthcare organizations should adopt approved secure communication systems. CMS guidance permits secure texting of patient information and orders in hospitals and critical access hospitals when the platform is HIPAA compliant and satisfies the Conditions of Participation. Organizations should therefore prohibit unapproved messaging for protected health information, require encryption and strong authentication, integrate orders and communications into the medical record when required, manage devices, and retain audit trails (CMS, 2024). Training should include realistic examples such as sending photographs, discussing patients in group chats, using voice assistants, and forwarding information to personal email accounts.

Cybersecurity communication should be continuous rather than limited to annual compliance modules. NIST recommends a risk-based approach that connects the HIPAA Security Rule with recognized cybersecurity controls. Organizations should conduct regular risk analyses, test incident-response procedures, review third-party vendors, apply least-privilege access, maintain backups, patch systems, use multifactor authentication where appropriate, and train workers to recognize phishing and social engineering (NIST, 2024). Leaders should explain that cybersecurity protects patient safety and continuity of care, not only regulatory compliance.

HIPAA communication must also address consumer applications that fall outside its scope. Patients should be told to review privacy policies, permissions, data-sharing practices, deletion procedures, advertising relationships, and breach-notification protections before using an app. Developers should use privacy-by-design principles, collect only necessary data, obtain meaningful consent, secure information in transit and at rest, and explain third-party disclosures in understandable language. The FTC's Health Breach Notification Rule, the FTC Act, state consumer-health privacy laws, and contractual obligations may apply even when HIPAA does not (FTC, 2024; ONC, 2026). Patient concerns identified in mHealth research show why transparency and usable privacy controls are necessary for trust and adoption (Alhammad et al., 2024).

Conclusion

All in all, HIPAA is well-intended, but the application and communication of the law can be difficult. Sensitizing stakeholders about the legislation and interpreting it as it applies to minors, state law, emergencies, electronic communication, cybersecurity, and consumer applications is a complex process. The solution is not to abandon HIPAA or leave privacy entirely to the states. Instead, healthcare organizations need accurate, scenario-based training; current state-law analysis; clear escalation procedures; secure communication platforms; risk-based cybersecurity; and honest explanations of where HIPAA does and does not apply. This approach can protect confidentiality without turning HIPAA into an unnecessary barrier to care, coordination, safety, and responsible innovation (HHS, 2023; NIST, 2024; ONC, 2026).

References

Alhammad, N., et al. (2024). Patients' perspectives on the data confidentiality, privacy, and security of mHealth apps: Systematic review. *Journal of Medical Internet Research, 26*, e50715. https://www.jmir.org/2024/1/e50715

Centers for Medicare & Medicaid Services. (2024, February 8). *Texting of patient information and orders for hospitals and CAHs*. https://www.cms.gov/medicare/health-safety-standards/quality-safety-oversight-general-information/policy-memos-states-and-cms-locations/texting-patient-information-and-orders-hospitals-and-cahs

Federal Trade Commission. (2024, April 26). *FTC finalizes changes to the Health Breach Notification Rule*. https://www.ftc.gov/news-events/news/press-releases/2024/04/ftc-finalizes-changes-health-breach-notification-rule

Legal Information Institute. (2026). *45 CFR § 160.203—General rule and exceptions*. Cornell Law School. https://www.law.cornell.edu/cfr/text/45/160.203

National Institute of Standards and Technology. (2024). *Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A cybersecurity resource guide* (NIST SP 800-66 Rev. 2). https://csrc.nist.gov/pubs/sp/800/66/r2/final

Office of the National Coordinator for Health Information Technology. (2026). *HIPAA for consumers*. https://healthit.gov/privacy-security/hipaa-basics/hipaa-consumers/

U.S. Department of Health and Human Services. (2023). *Personal representatives*. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/personal-representatives/index.html