HIPAA vs. HITECH vs. CURES ACT

A FRAGMENTED REGULATORY LANDSCAPE

Written By:

Elizabeth Notz McElhiney
MHA, CHPS, CPHIMS
Director of Compliance and Regulatory Affairs
Verisma

Wendy M. Lynch
J.D. Candidate, Expected 2023

verisma®

A FRAGMENTED REGULATORY LANDSCAPE

The United States has never established a universal health privacy law, relying instead on a patchwork of federal subject-specific laws and regulations working in conjunction with additional state-level privacy laws. Even within one level of government and a single industry, the oversight function is spread amongst multiple agencies and departments. A pertinent example is who oversees the disclosure of an individual's health data or protected health information (PHI). Most Americans would state that HIPAA protects their health information – which is only partially correct. The Office for Civil Rights (OCR) at the Department of Health and Human Services (HHS) would protect patients' information under the Health Insurance Portability and Accessibility Act (HIPAA). For disclosures to third parties, there may be limited protections from the Federal Trade Commission (FTC) if the disclosure is made to an app or no protections if the PHI travels outside of HIPAA entirely. These distinctions are often not communicated to patients or their personal representatives, leaving patients to navigate their own path through the varying protections granted by HIPAA, the Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009, and the 21st Century Cures (Cures) Act. These 3 significant laws each pertain to a specific, and different, class of PHI and offer appropriate safeguards within those parameters. Where the laws diverge, "bad actors" have found room to exist and offer to expedite the ROI process at low cost to third-parties and without the enumerated protections of HIPAA, HITECH, and the Cures Act.

This fragmented approach has further failed to provide adequate privacy protections for patients during the rapid evolution of health IT – particularly during the COVID-19 pandemic and after. A well-known phrase from the tech sector, "move fast, break things", speaks to a developer's mindset; a product or app is released quickly, and fixes can be rolled out as needed. The priority is getting to market and this approach was highly useful during the covid pandemic. This perspective is the inverse of traditional health IT which adopts a privacy-by-design approach and prefers to err on the side of caution. Healthcare has additional considerations, such as the inclusion of highly vulnerable populations like LGBTQIA+ patients, patients with substance use disorder diagnoses, and now patients seeking reproductive health care services or gender affirming care (in some states).

The contemporary political environment fails to provide any confidence that a federal privacy framework will be established at any point soon. Consequently, covered entities and business associates alike find themselves independently navigating an ever-evolving set of state and federal privacy laws. This whitepaper is intended to provide needed clarity on federal privacy laws and patient access regulations, how they interact, and how the existing patchwork of privacy laws fails to provide patients with comprehensive privacy protections. During the analysis, real-world examples will be included to demonstrate how third-parties leverage gaps in privacy protections or limited patient knowledge to obtain PHI for their own personal profit. These tactics include requesting excessive amounts of PHI, requesting a patient approve the disclosure of PHI without an expiration date, or moving sensitive information outside of the

protections of HIPAA. The paper will close with actionable insights on how to mitigate these ongoing risks to patient privacy.

THE FOUNDATIONS OF HEALTH PRIVACY, OR HOW WE GOT HERE

Federal privacy laws prior to the Health Insurance Portability and Accountability Act (HIPAA) of 1996 were narrow in scope and tended to pertain to a single issue or industry. Solove (2013) noted that while privacy legislation ensuring the privacy of cable TV and video rental records had been passed, there was no comparable effort made to secure an individual's medical records at the federal level. HIPAA was the first federal law to address the privacy and security of protected health information (PHI) as it moved between covered entities, patients, business associates, and third parties.

It may be easiest to visualize U.S. health privacy laws as a rambling older house; one where new additions, rooms, and wings were added when a family outgrew the existing building. In this analogy, the original house would be the first legislative efforts to protect patient health privacy 42 CFR Part 2. Additional space was needed to accommodate all PHI (HIPAA), ePHI (HITECH), and then EHI access (Cures Act). As often happens, the new sections are built in a contemporary manner and may be stylistically different from the whole residence. These 3 different laws all work together to ensure patient access to PHI and protect patient privacy; however, the manner and methods reflects the technology and needs of the day.

HIPAA

The original impetus for HIPAA is dependent on the individual writing its legislative and regulatory history. Some academics assert that the primary intent was to create a recognized, standard set of electronic transaction codes (Solove, 2013). Other authors argue the actual legislative intent was to enable continuity of health insurance coverage and to facilitate the transfer of that insurance coverage (Moore & Frye, 2019). Yet still others purport that the intent was always to provide for the protection of PHI from wrongful disclosure by healthcare providers (Sanger, n.d.). HIPAA is synonymous with medical records privacy protections in 2023.

The HIPAA Privacy Rule establishes a patient's rights regarding their PHI. These rights were previously not established under federal law and included:

1. The right to access their PHI (45 CFR § 164.524)
2. The right to amend their PHI (45 CFR § 164.526)
3. The right to restrict their PHI (45 CFR § 164.522)
4. The right to request an accounting of disclosures (45 CFR § 164.528)
5. The right to request alternative communications (45 CFR § 164.524)

Further requirements were found within each enumerated right. The most known set of requirements are the core elements and required statements of a HIPAA compliant authorization.

Figure 1: Sample Checklist for HIPAA Compliance – (45 CFR §164.524)

Authorization Component	Present?	
Core Elements	**Yes**	**No**
Patient Name and Identifier		
Patient Signature and Date		
Name of Person/Entity Releasing Information		
Name of Recipient		
Meaningful Description of Requested Information		
Purpose of Disclosure		
Relevant Expiration Date		

POA/Guardianship/LOE/Death Certificate + ARC		

Required Statements	**Yes**	**No**
Revocation Statement		
Redisclosure Statement		
Statement of Consequences/Effects of Not Signing		

It is worth discussing the specific core elements and requirements; these elements are intended to provide specific information for patients or their personal representatives. These elements have significant implications for the later discussion of third-party directives.

TABLE 1 - COMPARISON OF SAFEGUARDS PRESENT BY REQUEST METHOD

	Present On...		
Required Statement or Core Element	**Authorization**	**Directive**	**Verbal Request Under NPRM**
Meaningful description of requested information	✓		
Patient Signature and Date	✓	✓	
Expiration date (or event)	✓		
Right to revoke request (and how)	✓		
Notice of potential redisclosure	✓		
Notice that patient not required to sign	✓		

TABLE 2 - SPECIALLY PROTECTED INFORMATION RELEASED BY REQUEST METHOD

	Present On...		
Sensitive Information Automatically Released	**Authorization**	**Directive**	**Verbal Request Under NPRM**
HIV/AIDS		✓	✓
Sexually transmitted infections (STIs)		✓	✓
Genetic testing results		✓	✓
Substance use disorders (SUD)		✓	✓
Mental/behavioral health		✓	✓
Reproductive health		✓	✓

There is one specific portion of the HIPAA Privacy Rule that has had a disproportionate impact on the patient right to access debate. HHS made an additional effort to clarify who would constitute a personal representative under the Privacy Rule when the Department published "Guidance [for Professionals]: Personal Representatives" on their website. This guidance stated that "a person authorized (under state or other applicable law, e.g. tribal or military law) to act on behalf of the individual in making health care related decisions is the individual's "personal representative" and references §164.502(g) (US Department of Health and Human Services, 2013). Personal representative status may not be granted without documentation supporting the assertion, such as a healthcare power of attorney (HCPOA), letters of estate, or guardianship papers.

The HIPAA Privacy Rule also introduced the concept of the "minimum necessary" rule; this principle asserts that the minimum necessary information to respond to a treatment, payment, and operations (TPO) request (Solove, 2013). Under these rules, the overdisclosure of PHI in response to a request would be treated as a HIPAA violation.

HITECH Act

The HITECH Act was not intended to serve as a comprehensive update of the HIPAA Privacy and Security Rules. Congress' intent in passing the HITECH, along with its parent legislation, the American Reinvestment and Recover Act (ARRA) of 2009, was to support the American economy while simultaneously promoting and facilitating health care providers' adoption of EHR technology (Theodos & Sitting, 2020). The HITECH Act provided further clarification and restrictions on the disclosure and/or the sale of PHI at Sections §13402 through §13405; more specifically, that an individual may direct their PHI be sent to the either to an individual, or another person designated by the individual (Sanger, n.d.)

The third-party directive was the HITECH Act's effort to improve patient access to their PHI; the specific provision involved enumerating that a patient could obtain an electronic copy of any ePHI held by a covered entity. This provision was included to address both the American public's increasing adoption of email and willingness to use their email accounts to share PHI. Providers would not be required to purchase additional hardware, like scanners, to digitize paper or microfilm records. However, to the extent that such technology was already available, the records would need to be provided electronically.

A separate provision stated that a patient, or their personal representative, could direct a copy of their records to a designated individual or entity (§14305(e)). These third-party directives were meant to ensure that patients, and those standing in the patient's shoes, would be able to obtain ready access to ePHI.

The HITECH Act made provisions to further clarify the minimum necessary standard when it directed the HHS Secretary to provide guidance on the standard (Burde, 2011).

21st Century Cures Act

The Cures Act was intended to facilitate HHS' shift towards a value-based health system; patients would be able to direct, on demand, their EHI to another physician for a second opinion, transfer their records to a different hospital if dissatisfied with their care, or maintain a complete patient health record (PHR) (Bowen, Chamberlain, & James, 2020). The creation of an "app economy" also helped reduce barriers to patient access; patients no longer needed to request records in person or print/mail an authorization (McElhiney & Rodriguez, 2021). The establishment of the Trusted Exchange Framework and Common Agreement (TEFCA) in conjunction with API publishing requirements reduced the development time and costs for app developers (Morgan & Moriarty, n.d.).

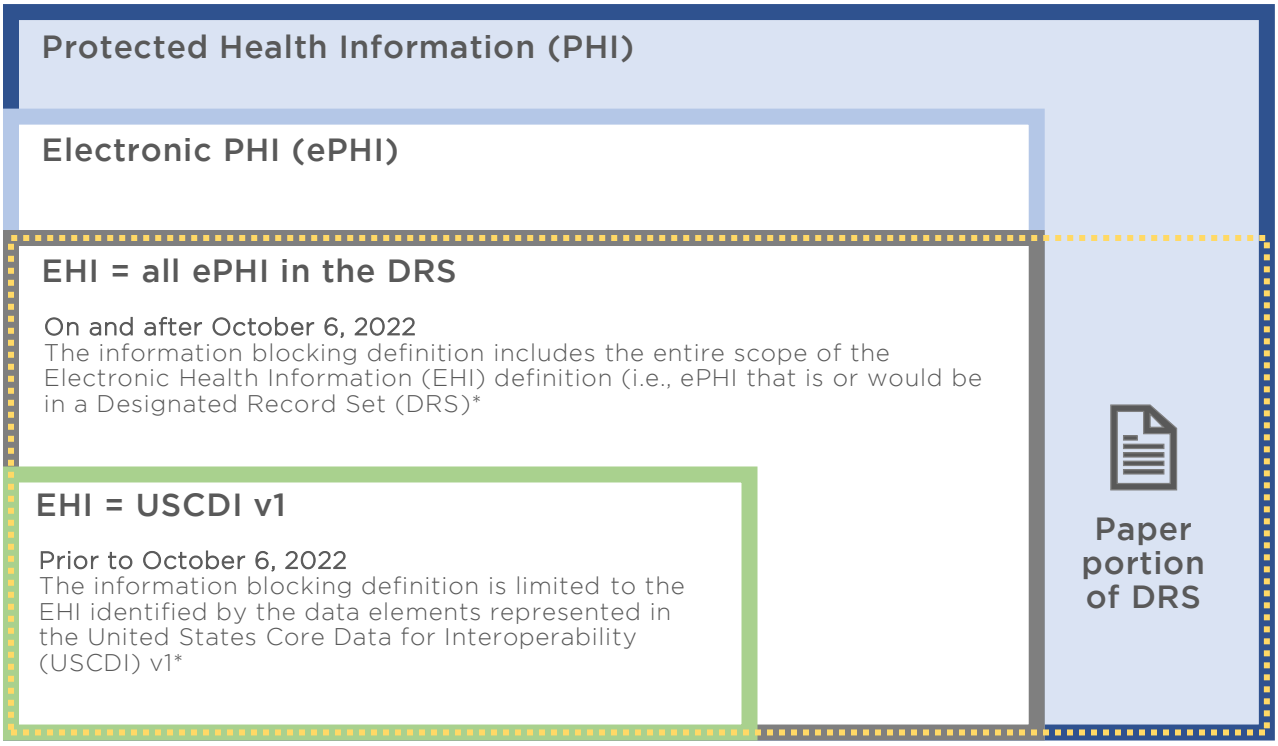
The Cures Act directed the Office of the National Coordinator for Health IT (ONC) and the Centers for Medicare & Medicaid (CMS) to generate regulatory policies to promote or incentivize the development and adoption of interoperable exchange between patients, covered entities, and other identified stakeholders (Bowen, Chamberlain, & James, 2020). Both the ONC Final Interoperability Rule and the CMS Final Interoperability Rule were published on March 9th, 2020. The ONC Final Rule has the most direct impact on a patient's right of access. ONC's recent proposed rule on appropriate provider disincentives clearly links the two organizations; penalties for committing information blocking result in a provider or ACO being unable to claim meaningful EHR use status for the purposes participating in MIPS and other CMS programs. These penalties would ultimately impact the covered entity/actor's reimbursement rates and ability to participate in some federal programs in the following year.

The specific subset PHI covered by the Cures Act was defined as EHI; initially EHI was defined as the US Core Dataset for Interoperability v1 and expanded to the ePHI in designated record set (eDRS) on October 6th, 2022. This change can appear to be of minimal importance and have a small impact on a covered entity's operational workflow. The expansion of available dataset is detailed in Figure 2; it assumes that the individual or organization recognizes that the designated record is more expansive than the legal medical record and would incorporate any application storing ePHI. This would include case management systems, EHR records for a specialty like radiation oncology, correspondence with insurance companies regarding prior authorizations, and any legacy EMRs that were part of acquiring another health care provider. Large health care organizations routinely have multiple EHR systems, current and legacy, in addition to numerous purpose-specific applications that do not flow into the EHR of record. These applications will need to be accessible under the Cures Act.

EHI was defined as the electronic designated record set due to the approved interoperability use cases –specifically, individual access and treatment. These use cases did not require a HIPAA compliant authorization to be implemented. Patients are entitled to access their full designated record set under HIPAA and could direct that information into an application or repository of their choice. Similarly, the exchange of EHI for treatment purposes is considered exempt under HIPAA as part of the "Treatment, Payment, and Operations" carveouts. The 21st Century Cures

Act has the similar vulnerabilities to misuse as the HITECH Act did – namely that third or fourth-party requesters seek to leverage patient access provisions to receive copies of EHI at low or no cost.

Figure 2: ONC infographic defining types of responsive record sets (Marchesini & Lipinski, 2021)



*EHI includes electronic protected health information (ePHI) to the extent that it would be included in a designated record set (DRS), regardless of whether the group of records is used or maintained by or for a covered entity or business associate. EHI does not include: psycholotherapy notes as defined in 45 CFR 164.501; or information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding 45 CFR 171.102.

Note #1: The infographic is not intended to depict the *actual* scope of each category of health information in a designated record set. For example, a DRS may consiste of no paper records and EHI identified by only the data elements represnted in the USCDI v1.

Note #2: Actors (45 CFR 171.102) not covered by HIPAA should familiarize themselves with this infographic and with HIPAA terms, and should asess what information they have that would be considered records that align with those included in the DRS. Such information is EHI for purposes of the information blocking definition.

PRIVACY BLIND SPOTS AND POTENTIAL FOR ABUSE

"HITECH Requests" and "PHR Requests" remove HIPAA's privacy guardrails

The HIPAA Privacy Rule was unapologetic about ensuring that patients were aware of their privacy rights; this included ensuring that an authorization would not be valid indefinitely, informing patients that they could (and how to) revoke a PHI request until it was acted upon, and reinforcing that PHI, once released, may fall outside the protections of HIPAA. The Privacy Rule further ensured that a HIPAA compliant authorization must be written in plain language so that the average citizen would understand the information provided. These stipulations demonstrated HHS' intent to put an informed individual at the center of their care and in control of their PHI.

Third-party directives result in PHI overdisclosure

Third-party directives may indirectly economically benefit requesters who elect to not utilize HIPAA compliant authorizations. A HIPAA compliant authorization will have a meaningful description of the information to be disclosed; third-party directives would be written in the voice of the patient and could authorize the disclosure of "all medical records" or "all dates of service".

Weaponization of the complaint process

Patient access is the unifying thread running through these three laws and their implementing regulations, despite their individual focus on disparate methods of accessing PHI. This is a laudable goal in and of itself. However, continued regulatory and legislative efforts strongly suggests that prior patient access efforts have fallen short of their goals. OCR has continued to publicize their investigations and settlement agreements to dissuade other healthcare providers from engaging in such behavior.

Third and fourth parties have taken notice of OCR's continued enforcement efforts and have accordingly sought to leverage the OCR complaint portal for their economic benefit. The ROI industry has witnessed multiple third- and fourth-party requesters engaging in deceptive and aggressive approaches when corresponding with healthcare providers. These requesters will repeatedly submit third-party directives to healthcare facilities and each resubmission will contain increasing amounts of self-described educational material. Ultimately, the requesting party will attach a completed OCR complaint form and letter detailing that the complaint will be filed should the request not be filled at a reduced fee of $6.50. On some occasions, these requesters will provide submitted OCR complaints but will offer to rescind the complaint if the physician or hospitals capitulate.

The misappropriation and weaponization of the OCR complaint portal is enabled by physician and hospital aversion to any potential complaint or investigation. Given OCR's commitment to

the patient access initiative, providers are aware that patient access complaints have taken on increased importance. Covered entities and business associates know that OCR investigations come at a significant economic and labor cost.

OCR has a broad remit and constrained resources; the misuse of the patient portal for pricing disputes has likely added thousands of complaints annually. It should be noted that these third and fourth-party requesters utilize the previously discussed third-party directive request process. These "bad actors" have begun to threaten health care providers by stating that the provider is engaging in information blocking under the 21st Century Cures Act. This would open a potential new complaint mechanism that can subverted for their purposes. The potential provider disincentives for information blocking behavior, as recently proposed in the Federal Register, may have a greater financial impact on providers than the existing OCR process.

CONCLUSION

Despite the passage of time and significant technological advancements, HIPAA has not undergone a comprehensive update since its Privacy and Security Rules became effective in 2003 and 2005 respectively. HIPAA has been accorded updates on an ad hoc basis when other significant health care legislation is introduced. Significant updates were contained in the Health Information Technology for Economic and Clinical Health (HITECH) Act, which was itself a constituent part of the American Reinvestment and Recovery Act (ARRA) of 2009 and the 21st Century Cures Act. The specific changes to patient access were introduced as they were ancillary to other larger policy aims within legislation.

This fragmented approach has unintentionally placed patient privacy at additional risk. Bad actors have engaged in misleading practices, weaponized the OCR's complaint process to ensure covered entities act on requests with no HIPAA safeguards in place, placed an ever-growing burden on OCR's limited resources due to the growing number of complaints, and have the potential to further erode patient privacy by selling patient PHI. These problems can only be addressed through a combined effort from the health care facilities, Congress, regulatory agencies, and other stakeholders.

Some commonsense steps to take include:

1. Create a Privacy Commission, akin to the one previously suggested by Senators Cassidy and Baldwin to determine what constitutes privacy, PHI, and define next steps to protect that information.
2. Pass legislation clarifying who constitutes a patient representative and is eligible to receive the patient rate.
3. Create a list of third parties who abuse the OCR complaint process – OCR should be able to conduct its important work and not be used to enforce a private industry's strategy.
4. Educate patients on their privacy rights – and when they apply.

ABOUT THE AUTHORS

Elizabeth McElhiney, MHA, CHPS, CPHIMS is Director of Compliance and Government Affairs for Verisma, a leading provider of Health Information Management (HIM) solutions, Ms. McElhiney is responsible for the administration of Verisma's privacy and compliance programs, working with clients to implement evidence-based best practices, and overseeing Verisma's thought leadership initiatives. Ms. McElhiney has worked in HIM and Release of Information for over 14 years; covering all areas of the industry from customer service to compliance. She currently sits on the Illinois Health Information Management Association (ILHIMA) Board of Directors and serves as a delegate to the American Health Information Management Association (AHIMA) House of Delegates. In addition, she is the current Secretary and CRIS Chairperson at the Association of Health Information Outsourcing Solutions (AHIOS). Ms. McElhiney holds a Bachelor of Arts in Political Science from Illinois Wesleyan University and a master's degree in health administration with a specialization in Health Informatics form Capella University.

Wendy M. Lynch is a Juris Doctor Candidate at the Thomas R. Kline School of Law of Duquesne University with a specialization in healthcare law. As a Legal Intern at UPMC Corporate Legal Department, Ms. Lynch focused on healthcare regulations, including the HITECH Act and Cures Act. Ms. Lynch's expertise in semantic interoperability developed during her role as Director of Market Segmentation for Population Health at Allscripts, showcasing her leadership in healthcare analytics and technology integration. Her work emphasized the importance of data analysis in healthcare.

DISCLAIMER

This whitepaper is for informational purposes only and does not constitute legal advice. The information contained in this whitepaper is based on the best available knowledge and research at the time of writing, but it may not be comprehensive, accurate, or up to date. The whitepaper does not represent the official views or opinions of Verisma or any of its affiliates. Readers should consult their own legal counsel before taking any action based on the information in this whitepaper. Verisma and its affiliates disclaim any liability for any loss or damage arising from or in connection with the use of this whitepaper or any of its contents.

WORKS CITED

Bowen, R., Chamberlain, S., & James, J. (2020, July 1). *Balancing Patient Access and Privacy: the impact on healthcare providers and their patients of March 9, 2020 Office of the National Coodinator (ONC) Final Rule.* Retrieved from AHIOS website: www.ahios.org

Burde, H. (2011). The HITECH Act - An Overview. *American Medical Association Journal of Ethics, 13*(3), 172-175.

Kiel, J. M. (2022). Data Privacy and Security in the US: HIPAA, HITECH, and Beyond. In U. Hubner, G. Mustata Wilson, T. Morawski, & M. Ball, *Nursing Informatics* (pp. 427-435). Springer, Cham. doi:https://doi.org/10.1007/978-3-030-91237-6_28

Marchesini, K., & Lipinski, M. (2021, December 20). *Say Hi to EHI - Health IT buzz.* Retrieved from healthit.gov: https://www.healthit.gov/buzz-blog/information-blocking/say-hi-to-ehi

McElhiney, E., & Rodriguez, C. (2021, December 7). *Access at the Expense of Privacy in the Emerging App Economy.* Retrieved from AHIOS website: www.ahios.org

Moore, W., & Frye, S. (2019). Review of HIPAA, Part 1: history, protected health information, and privacy and security rules. *Journal of Nuclear Medicine Technology, 47*(4), 269-272.

Morgan, S., & Moriarty, L. (n.d.). *21st Century Cures Act & The HIPAA Access Right.* Retrieved from ONC website: https://www.healthit.gov/sites/default/files/2018-12/LeveragingHITtoPromotePatientAccess2.pdf

Sanger, L. J. (n.d.). HIPAA Goes HITECH. *University of Houston Health Law Perspectives*.

Solove, D. J. (2013). HIPAA Turns 10: Analyzing the Past, Present, and Future Impact. *Journal of AHIMA, 84*, 22-28.

Tangari, G., Ikram, M., Ijaz, K., Kaafar, M. A., & Berkovsky, S. (2021, June). Mobile health and privacy: cross sectional study. *British Medical Journal, 373*(8296). doi:https://doi.org/10.1136/bmj.n1248

Theodos, K., & Sitting, S. (2020, December 7). Health Information Privacy Laws in the Digital Age: HIPAA Doesn't Apply. *Perspectives in Health Information Management, 18 (Winter)*.

US Department of Health and Human Services. (2013, September 19). *Guidance: Personal Representatives | HHS.gov*. Retrieved from HHS website: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/personal-representatives/index.html