NCVHS 2024 Report to Congress

On the Implementation of the Administrative Simplification Provisions of the Health Insurance Portability and Accountability Act (HIPAA) of 1996

A report of the

National Committee on Vital and Health Statistics

A public advisory body to the Secretary of Health and Human Services

U.S. Department of Health and Human Services

NCVHS

National Committee on Vital and Health Statistics

July 10, 2024

Honorable Mike Johnson
Speaker of the House of Representatives
H-232, The Capitol
Washington, D.C. 20515

Dear Mister Speaker:

I am pleased to transmit our 2024 Report to Congress on Implementation of the Administrative Simplification Provisions of the Health Insurance Portability and Accountability Act (HIPAA). In compliance with section 263, Subtitle F of Public Law 104-191, this report was developed by the National Committee on Vital and Health Statistics (NCVHS), the public advisory committee to HHS on health data, data standards, statistics, privacy, and national health information policy. It covers the period January 2021 through December 2023.

HIPAA was a visionary law that put the country on a path toward standardizing electronic health care transactions and protecting patients' health care information. At the time of its passage virtually all patient information was paper-based. Since then, much has changed.

In this year's Report to Congress, NCVHS identified challenges and opportunities that influence the continued advancement of the HIPAA administrative simplification provisions and actions taken to enforce the HIPAA Rules while protecting privacy and security. This report concludes by identifying emerging trends and challenges to standardize electronic health care administrative transactions and safeguard patients' sensitive medical information.

The Committee serves a unique role in providing a forum for stakeholders, including from the private sector and across the health care industry, to contribute real-world facts-on-the-ground input to inform the Committee's deliberations and recommendations to HHS, all of which are available online. As a Federal advisory committee to HHS, NCVHS also works in partnership with federal agencies and advisory bodies, including the Office of the National Coordinator (ONC) and its Health Information Technology Advisory Committee (HITAC) to ensure that the Committee's work is synergistic and in alignment with administration priorities.

We hope that you will find the Committee's 2024 report informative and useful. The Committee looks forward to continue advancing these important issues for the benefit of the nation's health system and ultimately patient care and well-being.

If your staff would like a briefing presentation on this or any of our past or anticipated activities, the Committee would be pleased to provide this information.

Sincerely,

/s/

Jacki Monson, Chair
National Committee on Vital and Health Statistics

CC: Secretary Xavier Becerra
HHS Data Council

Enclosure

Identical letter to:

The Honorable Mike Johnson
H-232, The Capitol
Washington, D.C. 20515

The Honorable Ron Wyden
Chairman
Committee on Finance
219 Senate Dirksen Office Building
United States Senate
Washington, D.C. 20510

The Honorable Patty Murray
President Pro Tempore
United States Senate
Washington, D.C. 20510

The Honorable Bernie Sanders
Chair
Committee on Health, Education, Labor and Pensions
428 Senate Dirksen Office Building
United States Senate
Washington, D.C. 20510

The Honorable Jason Smith
Chairman
Committee on Ways and Means
U.S. House of Representatives
1102 Longworth House Office Building
Washington, D.C. 20215

The Honorable Virginia Foxx
Chairwoman
Committee on Education and the Workforce
U.S. House of Representatives
2176 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Cathy McMorris Rodgers
Chair
Committee on Energy and Commerce
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, D.C. 20215

Cc: The Honorable Xavier Becerra
HHS Data Council Co-Chairs

The National Committee on Vital and Health Statistics

The National Committee on Vital and Health Statistics (NCVHS) serves as the statutory [42 U.S.C. 242(k)] public advisory body to the Secretary of the Department of Health and Human Services (HHS) in the areas of health data, standards, statistics, national health information policy, and the Health Insurance Portability and Accountability Act (HIPAA). In that capacity, the Committee provides advice and assistance to HHS and serves as a forum for interaction with relevant private-sector groups on a range of health data issues. The Committee is composed of 18 individuals from the private sector who have distinguished themselves in the fields of health statistics, electronic interchange of health care information, privacy and security of electronic information, population-based public health, purchasing or financing health care services, integrated health information systems, health services research, consumer interests in health information, health data standards, epidemiology, and the provision of health services. Sixteen of the members are appointed by the Secretary of HHS for terms of 4 years each. Two additional members are selected by Congress. See the NCVHS membership roster in Appendix C or visit https://ncvhs.hhs.gov/.

This report was prepared by NCVHS members and staff in collaboration with Patricia MacTaggart, MBA, MMA, and Denise E. Love, BSN, MBA, consultant writers with Rose Li & Associates.

NCVHS Membership
Jacki Monson, JD, **NCVHS Chair**
Angela M. Alton, MPA
Tammy Feenstra Banks, MBA, FACMPE
Denise Chrysler, JD
Catherine Molchan Donald, MBA
Jamie A. Ferguson
Michael L. Hodgkins, MD, MPH
R. Lenel James, MBA
Debra Strickland, MS
Steven Wagner, MBA
Valerie J.M. Watzlaf, PhD, MPH, RHIA, FAHIMA
Wu Xu, PhD

Naomi Michaelis, MPA, **NCVHS Executive Secretary/Designated Federal Officer**
National Center for Health Statistics, Centers for Disease Control and Prevention, HHS

Sarah Lessem, PhD, **NCVHS Executive Staff Director**
Office of Science and Data Policy, Office of the Assistant Secretary for Planning and Evaluation, HHS

Lorraine Tunis Doo, MPH, **Lead Staff to the Subcommittee on Standards**
Senior Policy Advisor
Health Informatics and Interoperability Group, Office of Burden Reduction and Health Informatics
Centers for Medicare & Medicaid Services, HHS

Maya A. Bernstein, JD, **Lead Staff to the Executive Director, NCVHS, Lead staff to the Subcommittee on Privacy, Confidentiality & Security**
Senior Advisor, Privacy Policy, Office of the Assistant Secretary for Planning and Evaluation, HHS

Table of Contents

Executive Summary

The National Committee on Vital and Health Statistics (NCVHS) is charged with assisting and advising the Secretary of the Department of Health and Human Services (HHS) on health data, statistics, privacy, information security, national health information policy, and the Department's strategy to best address these issues. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 further directed NCVHS to report to Congress regularly on the implementation status of the HIPAA administrative simplification provisions. This report summarizes actions related to HHS' strategy to standardize electronic health care administrative transactions and safeguard patients' sensitive health information during the 2021-2023 reporting period.

The report provides (1) context for the challenges and opportunities that influence the continued advancement of the HIPAA administrative simplification provisions, (2) actions taken to simplify administrative processes, protect privacy and security, and enforce the HIPAA Rules during this 3-year period, and (3) emerging trends and challenges.

Health IT and Data Policy, Standards and Models

Section I of the report will address the evolution of Health Information Technology (Health IT) and digital innovations since the enactment of HIPAA.

Progress Toward Implementing HIPAA Administrative Simplification—2021-2023

Section II will provide an overview of progress toward implementing HIPAA Administrative Simplification Provisions and Privacy Rules in the 2021-2023 reporting period, including barriers and opportunities identified by NCVHS in the HIPAA standards development and adoption processes. The Section also discusses some actions taken by NCVHS to address significant HIPAA Administrative Simplification provisions and privacy including:

1. NCVHS monitored the progress of the Centers for Medicare & Medicaid Services' (CMS) regulatory activities, including the release of two proposed rules for HIPAA standards: one that would update HIPAA pharmacy standards and one that would adopt standards for attachments. CMS conducted rulemaking in other areas not pertaining to HIPAA standards that may in the long term have an impact on HIPAA.
2. NCVHS issued a "Request for Comment" and convened a national meeting to inform the Committee's action on key unresolved issues related to compatibility across existing and proposed versions of standards, limited return on investment data, and bundling of transaction versions.
3. NCVHS made recommendations to HHS to Improve Public Health Data Sharing by clarifying that all American Indian/Alaska Native entities meet the definition of "public health authority" in 45 C.F.R. §164.501 and should be able to access data on the same basis as any other public health entity.
4. NCVHS made recommendations to HHS to conduct rulemaking for proposed Eligibility and Benefit, Claims Status, Electronic Payment, and Remittance Advice Operating Rules;

take action for future adoption of the International Classification of Diseases (ICD), eleventh edition (ICD-11) in the United States; require covered entities (CEs) to implement the specification in the HIPAA Security Rule or to adopt a documented reasonable alternative; adopt minimum cyber hygiene requirements; provide additional cybersecurity support and guidance to under-resourced entities; and develop a national governance strategy specific to Public Health Emergencies to increase trustworthiness in data collectors.

Emerging Trends and Challenges for Congress and Other Leaders to Consider 2024-2025

Section III will highlight three focus areas for Congress and HHS to consider as ways to support innovation while providing guardrails that limit unintended consequences: (1) standardization for interoperability, (2) cybersecurity, and (3) monitoring emerging technologies.

As health care evolves, so does the need for Health IT and data sources. Congressional and HHS efforts to standardize electronic health care administrative transactions and safeguard patients' sensitive medical information should consider addressing the demands and dependencies that a digital health care ecosystem requires. Foundational to the optimization of these drivers and dependencies is the awareness that health care, technology, and data constantly change, requiring updated standards to appropriately act today and in the future. These include:

1. **Standardization for Interoperability**: Update standards including those adopted under HIPAA to meet current and future business needs, which includes creating a system and structure for evaluation of administrative transaction costs and value and preparing for ICD-11. Update technical guidance on deidentification of essential health data, including public health data, resulting from changes in data collection practices, the availability of ever larger and more complex data systems, and technology advancements. Include lesser resourced entities in federal discussions.

2. **Cybersecurity:** Implement the specifications in the Security Rule to include minimum cybersecurity hygiene requirements and predictive modeling to be inclusive of the risk analysis framework. Evaluate the level of compliance by HIPAA CEs and their business associates with the HIPAA Security Rule and increase enforcement. Help small health care entities and third parties with the greatest need in meeting the enhanced minimum-security requirements. Provide federal guidance on how to conduct a deeper assessment of safety and security issues including solutions related to artificial intelligence (AI).

3. **Health IT and Digital Innovations:** Develop a roadmap that addresses data and infrastructure guardrails and provides federal guidance on how to conduct a deeper assessment of Health IT and digital innovations, including AI, Fast Healthcare Interoperability Resources® (FHIR®), quantum computing, and other innovations. Develop and detail a national framework that addresses data and infrastructure related to the timely exchange of standardized health data to other health authorities and models for integrating HIPAA and non-HIPAA data. Ensure frameworks address privacy and security implications of AI.

Introduction and Report Overview

The National Committee on Vital and Health Statistics (NCVHS) serves as the statutory public advisory body to the Secretary of the Department of Health and Human Services (HHS) on health data, statistics, privacy, and national health information policy and the Health Insurance Portability and Accountability Act (HIPAA). [1] The Committee advises the HHS Secretary, reports regularly to Congress on HIPAA implementation, and serves as a forum for interaction between HHS and interested private-sector groups on a range of health data issues.[2] Since 1996, NCVHS has issued periodic Reports to Congress on the status of HIPAA implementation in addition to making numerous recommendations to the Secretary developed through extensive consultations with health care industry stakeholders. This Report to Congress, mandated under HIPAA,[3] is a progress report from January 1, 2021, through December 31, 2023, on HHS activities related to electronic health care administrative transactions and safeguarding of patients' sensitive health information.

The report provides (1) context for the challenges and opportunities that influence the continued advancement of the HIPAA administrative simplification provisions, (2) actions taken to simplify administrative processes, protect privacy and security, and enforce the HIPAA Rules during this 3-year period, and (3) emerging trends and challenges.

[1] Congress enacted the statutory basis for the National Committee on Vital and Health Statistics as part of Public Law 93–353, the Health Services Research, Health Statistics, and Medical Libraries Act of 1974. Now codified at 42 U.S.C. § 242k(k), the law established NCVHS as an advisory committee to the Secretary of the former Department of Health, Education, and Welfare (now HHS), expanded its membership from 12 to 15 members, and considerably amplified its area of interest in health statistics. Subsequently, the Health Services Research, Health Statistics, and Health Care Technology Act of 1978 (Public Law 95–623) further broadened the scope of activities of the Committee in the areas of environmental and epidemiological activities and in matters concerning the Cooperative Health Statistics System. The Health Insurance Portability and Accountability Act (HIPAA), Public Law 104–191, 110 Stat. 1936 (Aug. 21, 1996), assigned further obligations to NCVHS in sections 262, at 110 Stat. 2024 (codified at 42 U.S.C. §§ 1320d-1), section 263 at 110 Stat. 2031, and 264 at 110 Stat. 2033-34) regarding health information privacy and health data standards.

[2] Learn more at About NCVHS.

[3] 42 U.S.C. § 242k(k)(7), added by section 262 of HIPAA.

I. Health Information Technology and Data Policy, Standards and Models That Influence the Continued Advancement of the HIPAA Administrative Simplification Provisions

Since HIPAA's enactment, U.S. health care delivery models have evolved to include in-person, virtual, and hybrid approaches. As care models have evolved, so has the need to improve the quality of health care, reduce inequities in health care delivery, and reevaluate how evolving technology uses health care data. Cybersecurity is of vital importance within health care because of an increased dependency on technology and the value of personal information. Additionally, payment models have changed to focus on incentives to improve clinical outcomes. These redesigned models drive the need for actionable information based on accurate, private, secure, and timely data within the information technology (IT) environment.

The electronic exchange of administrative and clinical data is not limited to the transactions[4] that HIPAA covers. Health data exchange has become increasingly important for taking care of the whole patient, where they want and when they want. These changes were not contemplated in the original HIPAA rule. Data sharing now encompasses social and behavioral services, public health, cost, quality assessment, and research, which supplement the purpose of the HIPAA administrative and financial transactions to reduce administrative costs. Transaction processing technology has migrated away from mainframe computing and batch processing for which HIPAA standard transactions were designed. Data exchange is now accomplished through new technologies and shared with a broader array of actors, adding complexity and pushing the limits of HIPAA's privacy and security protections.

Emerging Health IT and digital innovations introduce advantages and disadvantages to health care, as does the introduction of artificial intelligence (AI). The evolution of Health IT and data standards introduce the ability to address social determinants of health (SDOH) data but can still

---

[4] Section 262 of HIPAA amended Title XI of the Social Security Act to add the provisions on administrative simplification. These included nine transactions for which the Secretary is required to adopt standards:

(A) Health claims or equivalent encounter information;
(B) Health claims attachments (no standard adopted yet);
(C) Enrollment and disenrollment in a health plan;
(D) Eligibility for a health plan;
(E) Health care payment and remittance advice;
(F) Health plan premium payments;
(G) First report of injury (no standard adopted yet);
(H) Health claim status; and
(I) Referral certification and authorization.

Section 1104(b)(2) of the Patient Protection and Affordable Care Act (hereafter ACA), Public Law 111–148, 124 Stat. 915, added an additional transaction:

(J) electronic funds transfers.

Social Security Act, § 1173, codified at 42 U.S.C. § 1320d–2.

result in data gaps. The adoption of new data standards and increasing interoperability have created opportunities and challenges not previously encountered for administrative simplification, privacy, and security. Other opportunities and challenges include the move toward cloud computing, the eventual transition from International Classification of Diseases (ICD) tenth edition (ICD-10) and its U.S. edition ICD-10 Clinical Modifications to ICD-11 in the United States, privacy related to reproductive health, the HIPAA transactions process, and the risks posed by cybersecurity. The following section discusses the risks and opportunities posed by each of these areas.

Health IT and Digital Innovations

Emerging Health IT and digital innovations have expanded modalities for the delivery of care and provided tools for use by health care providers and consumers, for example, Internet of Medical Things, mobile devices, telehealth, remote monitoring, fifth-generation wireless networks (5G), use of nanotechnology, cloud computing, AI, and robotic process automation. However, many of the data sources and types of data transports from one system to another are not covered by HIPAA (e.g., data collected and exchanged from mobile devices and wearables that is not protected health information [PHI] under HIPAA),[5] which creates potential risks. Because of their capacity to collect and use large amounts of sensitive health data, these new modalities may bring privacy, security, algorithmic bias, and other risks.

Emerging technologies paired with the appropriate use of data can support health care delivery and decisions. However, there are privacy and security risks based on lack of transparency about the sources of data used and software shortcomings such as the potential for algorithm development bias. Algorithmic bias may be introduced either because data inputs are incomplete, inaccurate, or non-representative data; an algorithm is trained on limited, non-representative data; or the computational model is programmed in a way that is biased. These factors produce system and repeatable errors.

Assisted, Augmented, and Automated AI, Machine Learning, Deep Learning, Including Natural Language Processing and Generative Pre-Trained Transformers

The need for transparency, oversight, and accountability in technical applications is critical to managing the explosive deployment of AI technologies. AI presents opportunities for innovation and improvements in research, clinical diagnostics, administrative simplification, and pharmaceutical developments. It has the potential to alleviate clinician burnout associated with documentation by reducing the burden of implementing upgraded or new standards, code sets, and identifiers for example, by adapting text to various reading levels, audiences, and languages. While AI also introduces new risks including lack of transparency, bias and discrimination, social manipulation, increased liability, loss of organizational credibility, compromise to privacy, and security, legal, and ethical risks, it can also be used to mitigate some of those same risks by quickly identifying threats or errors and suggesting mitigation opportunities.

---

[5] NCVHS, "Health Information Privacy Beyond HIPAA: A 2018 Environmental Scan of Major Trends and Challenges" (Dec. 13, 2017).

Data Standards to Share Social Determinants of Health Data

Standardized sources of SDOH data to address non-medical factors (environmental, demographic, economic, and others) are essential to identifying and managing the health of vulnerable populations and patients at risk for poor health outcomes. The United States Core Data for Interoperability (USCDI) is a standardized set of health data classes (an aggregation of data elements by common theme i.e., types of illnesses) and constituent data elements for nationwide, interoperable health information exchange.[6] Versions 2 and 3 of the USCDI added health equity–related data elements to improve the collection and exchange of SDOH data. This update means that information about a person's SDOH may be documented in the health records. Eventual use of certain exchange standards can lead to real-time access to data, a reduction in reporting burden, alignment improvement between Electronic Clinical Quality Measures, and use of the data to make decisions about a patient's care. A lack of incentive for providers to collect SDOH data and variation in data collection results in continued data gaps and outcome disparities, creating barriers to care. New Application Programming Interfaces (APIs) increase patient access to their data but also introduce risks to patients, providers, and payers. These APIs provide a way to exchange clinical and SDOH data and must meet certain technical requirements, including use of the Fast Healthcare Interoperability Resources® (FHIR®), a Health Level Seven International® (HL7®) standard and implementation guide, enabling better integration and interoperability in health care systems.

Role of Information and Technology in Addressing Health Inequities and SDOH

To understand the non-medical and social factors affecting a patient, providers must collect and exchange data about patients and their community, including race and ethnicity, sexual orientation, socio-economic conditions, and environment. This information allows providers to better understand their patients' situation and find ways to improve their health care outcomes. The persistence of data silos across the health care system hinders the transfer of data across public health entities at all levels of government.

The COVID-19 pandemic exposed the need for greater clarity on the collection, use, and exchange of public health surveillance data in a Public Health Emergency. Variation in standards and reporting requirements at governmental levels point to the need for a national governance strategy including a framework for collection and analysis of SDOH data for HIPAA and non-HIPAA entities. The HIPAA Privacy Rule permits covered entities (CEs) to disclose PHI, without authorization, to public health authorities who are legally authorized to receive such reports for the purpose of preventing or controlling disease, injury, or disability.[7] However, the lack of understanding of these authorities and variations in the capabilities of some providers contributed to delayed agreements or denied requests to appropriately share public health data. The collection of SDOH data in a standard way by HIPAA CEs will improve clinical decision-making as well as the secondary data that are repurposed to support policy and research. With more granular and expansive data, vulnerable populations can be represented in statistical data,

[6] HHS, Office of the National Coordinator for Health IT, United States Core Data for Interoperability (USCDI) (July 2020).
[7] HHS, Office for Civil Rights (hereafter OCR), "Disclosures for Public Health Activities" (April 3, 2003).

and clinical decision-makers may be empowered to act. A national framework could provide clarity on timely exchange of standardized public health data to other public health authorities (state, tribal, local, territorial), and models for integrating HIPAA and non-HIPAA data.

Although public health data disclosure may have a disproportionate impact on some populations, not collecting or sharing the data risks perpetuating health inequities. In 2017, NCVHS recommended that the Office for Civil Rights (OCR) update its technical guidance on de-identification and become more vigilant as changes in data collection practices and technical advancements continue.[8]

Interoperability

With the passage of the 21st Century Cures Act, Congress required HHS to promulgate regulations to improve interoperability, among other requirements. The Office of the National Coordinator for Health Information Technology (ONC) and Centers for Medicare & Medicaid Services (CMS) have published rules to meet the requirements of this Act, several of which are in effect. These regulations address the adoption of HL7 FHIR-based standards that support interoperable data exchange between provider and payers and enable patients to securely access their data. Together, these regulations will impact the speed and degree of operational use across systems.[9] Additionally, the Act's Trusted Exchange Framework and Common Agreement (TEFCA) establishes a baseline for health information sharing among individuals and all HIPAA CEs and non-HIPAA CEs. TEFCA's Common Agreement, an agreement between the Recognized Coordinating Entity and Qualified Health Information Networks, establishes the infrastructure to securely share data. The Common Agreement requires that non-HIPAA CEs that participate in TEFCA protect PHI in the same manner as a HIPAA CE.

Equitable technology access is also a high priority across rural and other hard to reach areas ("the last mile"). Rural, small, and mid-sized practices, community health centers, and public health organizations are too often left behind, with interoperability initiatives resulting in medical knowledge not being equitably available to all end users.[10] Lesser resourced stakeholders struggle to comply with regulations and other requirements due to workforce limitations, lack of affordable broadband connectivity, and other resource constraints. There is a high-priority need for continued inclusion of these organizations in federal discussions and consideration for the allocation of resources to assist these organization moving forward.

Cloud Computing

Rather than the health care organizations owning their computing infrastructure or data centers, health care organizations can now lease computing storage or processing with remote cloud service providers. This ability enables organizations to expand computing and analytic

---

[8] Letter from William W. Stead, Chair, NCVHS, to Secretary Price, "Recommendations on De-identification of Protected Health Information under HIPAA" (Feb. 23, 2017).
[9] HHS, Office of the National Coordinator for Health IT (hereafter ONC), Final Rule, "Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing," 89 Fed. Reg. 1192 (Jan. 9, 2024).
[10] Bradford William Hesse, "Role of the internet in solving the last mile problem in medicine," *Journal of Medical Internet Research*, 2019 Oct; 21(10): e16385. doi: 10.2196/16385.

infrastructure and leverage the latest technologies. Although cloud computing is less vulnerable than on-premise infrastructure, privacy concerns remain because of the sensitive nature of health information and security risks related to cloud-based models. Users of cloud computing support should be vigilant in maintaining continuing compliance with the strict security requirements for the health care sector or by federal standards. The potential privacy and security risks may cause organizations (cloud service providers) to be reluctant to share information or provide access to their infrastructure with outside vendors.

ICD-11

The latest version of the International Classification of Diseases (ICD) is the eleventh edition (ICD-11). It was adopted by the World Health Assembly (WHO) in 2019 and became available for use globally on January 1, 2022. The 64-member countries of WHO are currently in different stages of implementation of ICD-11. ICD-11 leverages modern information technologies to automate and standardize clinical and patient-centered information. ICD-11 could enable automated documentation and coding of clinical detail derived from electronic health records (EHRs), reducing clinician coding and documentation burdens. Automated documentation, in turn, could improve metrics that rely on codes, such as public health reporting, clinical quality assessment, health services, and outcomes research. However, if not planned well, the regulatory adoption of ICD-11 could result in costly, uneven implementation across the industry, creating risks such as increased cost to providers and public agencies. There also will be costs for education and training on changes to coding policies and procedures. Additionally, research, planning, and engaging stakeholders to promote adoption of ICD-11 in the United States could be delayed.

Privacy Related to Reproductive Health

"The Supreme Court's decision in Dobbs v. Jackson Women's Health Organization[11] (Dobbs) makes it more likely than before that individuals' PHI [protected health information] may be disclosed in ways that cause harm to the interests that HIPAA seeks to protect."[12] The new legal environment is likely to impact "access to lawful health care and full communication between individuals and health care providers" and "increase the potential for uses or disclosures about an individual's reproductive health to undermine access to and the quality of health care generally."[13] The Dobbs ruling has resulted in the reactivation of reproductive health laws in some states, and new state privacy laws have introduced uncertainty and burden across HIPAA CEs and unintended consequences for public health activities. It has elevated the need for review of deidentification practices and redisclosures (the disclosure of PHI that was first provided to a HIPAA CE and then shared outside of that HIPAA CE), including how data are exchanged through Health Information Exchanges. The actions of state legislatures following the Dobbs ruling may influence the ways that health care providers document and code certain

[11] 597 U.S. 215 (2022).
[12] HHS, Notice of Proposed Rulemaking, "HIPAA Privacy Rule To Support Reproductive Health Care Privacy," 88 Fed. Reg. 23506, 23507 (April 17, 2023).
[13] *Ibid.*

clinical diagnoses and procedures in EHRs, which may decrease data accuracy, quality, and the safety of patients.

HIPAA Transactions Standards Process

HIPAA standards have transformed the industry by reducing administrative burden through the electronic exchange of certain business and financial transactions.[14] However, updates to some HIPAA standards and the development, recommendation, and adoption of HIPAA transaction standards and operating rules have not kept pace with the evolving business, operations, and technology requirements of HIPAA CEs. Health IT standards are evolving to support more expansive health data flows than are currently encompassed under HIPAA. The evolution in Health IT standards has resulted in data gaps in EHRs (such as race/ethnicity/SDOH data) and has led to calls by industry and other stakeholders for a strategic vision and modernization of HIPAA. The NCVHS Predictability Roadmap project[15] was undertaken to address the need for revising the HIPAA transactions standards development, recommendation, and adoption process. Past events (prior to the reporting period) included a workshop, listening session, and CIO forum, which informed the submission of actionable recommendations sent to HHS in 2018. The current workplan on harmonization of standards is a follow on to those earlier activities.

Cybersecurity

Health care cybersecurity incidents continue to dramatically increase in frequency and magnitude. Cybersecurity incidents have consequences for consumer health and safety, the delivery of care and treatment, and costs as the number of PHI breaches increases. If existing HIPAA regulatory security controls were implemented and followed diligently by HIPAA CEs, business associates (BAs), subcontractors, and vendors, it could prevent many health care cyber incidents and data breaches.[16] Poor security practices increase the vulnerability of patient information in health information systems. When breaches of health information occur, they often have serious consequences for organizations and consumers, including reputational and financial harm and erosion of patient trust.

Many security issues can be mitigated with proper risk management and risk analysis performed not only by HIPAA CEs but by BAs and other vendors and contractors.[17]

---

[14] By reducing the need for proprietary means of exchange of data between trading partners, the implementation of HIPAA standards across the industry paved the way for seamless automation of claims processing, eligibility verification, payment, and other administrative processes. HIPAA applies to HIPAA CEs (i.e., health plans, health care clearinghouses, doctors, hospitals, and various other health care providers).

[15] NCVHS, Subcommittee on Standards, "Improving Health Care System Efficiency by Accelerating the Update, Adoption, and Use of Administrative Standards and Operating Rules: A Brief History and Draft Recommendations" (Draft, Sept. 2018).

[16] *View generally,* letter from Jacki Monson, Chair, NCVHS, to Secretary Becerra, "Recommendations to Strengthen Cybersecurity in Health Care" (hereafter Cybersecurity Letter, May 10, 2022) and letter from Jacki Monson, Chair, NCVHS to Secretary Becerra, "Recommendations to Strengthen the HIPAA Security Rule" (hereafter Security Rule Letter, Nov. 23, 2023).

[17] *Ibid.*

The Health IT and digital innovations discussed above will continue to have an impact on HIPAA administrative simplification, privacy, and security and overall health care.

II. 2021-2023 HIPAA Administrative Simplification Provisions —Progress and Activities

This section provides an overview of progress and activities related to the HIPAA administrative simplification provisions including transactions, code sets, operating rules, and the Privacy, Security, and Breach Notification Rules during the 2021-2023 reporting period. The section discusses some NCVHS recommendations and includes industry survey data showing trends in HIPAA adopted transaction usage and breaches of PHI reported to OCR.

A. HIPAA Standard Transactions and Medical Code Set Standards and Operating Rules 2021-2023

NCVHS has advised HHS on the adoption and implementation of standards, identifiers, code sets, and operating rules since the passage of HIPAA in 1996.[18] In 2010, the Patient Protection and Affordable Care Act (ACA) established a new requirement to name an entity to author operating rules for each of the adopted HIPAA standard transactions. The operating rules explain how to use an implementation specification when the specification itself does not. HHS designated CAQH CORE (Committee on Operating Rules for Information Exchange) to serve in that capacity for certain administrative transactions and designated the National Council for Prescription Drug Programs (NCPDP) as the authoring entity for operating rules for pharmacy transactions. As health information needs and technology evolve, data flows are more expansive than contemplated under HIPAA and other federal legislation, leading to calls by industry and other stakeholders for a strategic vision and modernization of the HIPAA standards update[19] and adoption processes.

In June 2021, NCVHS (in consultation with industry, ONC, and CMS), proposed a framework and workplan, *Convergence 2.0,* to collaborate with governmental and industry stakeholders and develop actionable recommendations to modernize the standards adoption framework and harmonize clinical, public health, and other standards with HIPAA standards.[20] The recommendations made during 2021-2023 were in response to new standards proposals, evolving technological and information needs, and recognized-opportunities to bring HIPAA

---

[18] The standards are those adopted by HHS under HIPAA. The most recent versions of the standards were adopted on January 16, 2009 in a final rule titled "Health Insurance Reform; Modifications to the Health Insurance Portability and Accountability Act (HIPAA) Electronic Transaction Standards," 74 Fed. Reg. 3296.

[19] HHS has adopted standards for transactions under HIPAA, which are: Claims & Encounters, Claims Status, Coordination of Benefits, Eligibility, Enrollment, Claims Payment (Electronic Remittance Advice), Electronic Funds Transfer, Prior Authorization/Services Review, and Premium Payment. The X12 Version 005010 is the currently adopted version of all the X12 HIPAA standards. Version D.0 is the version of the pharmacy standard.

[20] NCVHS, Standards Subcommittee, "Project Scope: Standardization of Information for Burden Reduction and Post-Pandemic America (Convergence 2.0)" (June 21, 2021).

transaction standards into optimal configuration to gain the efficiencies envisioned in the original HIPAA legislation. We believe the NCVHS recommendations will provide useful insights to HHS as it continues its work with voluntary industry Standards Development Organizations (SDOs), other industry organizations, and Federal agencies toward streamlining the standards review process and other relevant process improvements. Industry adoption and use of named HIPAA transaction standards has been steadily increasing.[21]

Table 1 is a snapshot of the uptake of eight HIPAA named administrative standards[22] from 2013 to 2023 as reported by CAQH in the annual CAQH Index report.[23] By 2023, automated health care claim submissions (as reported by survey participants) represented 98% of the total number of covered submissions. Automated eligibility transactions represented 94% of the total eligibility transactions. Prior authorization (31%) is slowly shifting from payer portals and manual processes to automated transactions. Although HHS has not yet adopted a standard for health care attachments,[24] the table shows voluntary usage of attachments is below 30%. Transactions with lower implementation rates are those for which challenges may have been identified by survey participants or do not meet industry business needs. The Claim Payment/Electronic Fund Transfer (EFT) transaction, currently at 73% implementation, poses unique implementation challenges (e.g., fees charged by vendors and payers and certain contract issues). The implementation of EFT transactions has decreased by 3% over the past 2 years.[25]

[21] CAQH has conducted a voluntary annual survey of payers and providers since 2011. The results of this survey are used to calculate the CAQH Efficiency Index©, which tracks industry implementation of the HIPAA administrative transactions (excluding pharmacy standards and premium payment). Past CAQH Index reports may be found on the CAQH website.

[22] HHS Guidance Portal, "Adopted Standards and Operating Rules" (Aug. 2, 2020).

[23] CAQH, "2023 CAQH Insights Report: A New Normal: How Trends From the Pandemic are Impacting the Future of Healthcare Administration" (2024).

[24] Attachment transactions include additional information submitted with claims for payment, claim appeals, or prior authorization, such as medical records to support a claim or to explain the need for a procedure or service.

[25] The Electronic Remittance Advice (ERA) is an electronic version of a payment explanation submitted by a health plan to a provider that explains the payment a provider receives for a service claim. If a claim is denied or the payment adjusted, the ERA would contain the required explanations. CAQH CORE, "Phase III CORE 370 EFT & ERA Reassociation (CCD+/835) Rule version 3.0.0" (June 2012). The most recent CORE Payment & Remittance EFT Enrollment Data Rule identifies challenges faced by providers due to the variance of processes and data elements requested when enrolling in EFT with a health plan, including variations in data terminology used for the same semantic concept (e.g., Routing Number" vs. "Bank Routing Number"), resulting in inconsistent data entry that requires manual follow-up and resubmissions. CAQH CORE, "Payment and Remittance EFT Enrollment Data Rule, Version PR.2.0" (March 2024).

Table 1. Percent Industry Implementation of Transaction Standards Adopted Under HIPAA

Percent Industry Implementation of Transaction Standards	2013	2016	2017	2018	2019	2020	2021	2022	2023
Health care claim submission	90%	94%	95%	96%	96%	96%	97%	97%	98%
Eligibility for a health plan	65%	76%	79%	85%	84%	84%	89%	90%	94%
Coordination of benefits	NR	56%	75%	80%	86%	89%	87%	91%	90%
Health care claim status inquiry/response	48%	63%	69%	71%	70%	72%	68%	72%	74%
Claim payment (EFT)	50%	62%	60%	63%	70%	71%	76%	75%	73%
Remittance advice	43%	55%	56%	48%	51%	57%	64%	83%	88%
Prior authorization	NR	18%	8%	12%	13%	21%	26%	28%	21%
Attachments (no std adopted as of 2022)		NR	6%	NR	20%	22%	21%	24%	29%

During this reporting period, HHS issued two proposed rules that were relevant to the Committee's purview related to HIPAA administrative simplification transaction standards. The first would update NCPDP pharmacy standards from the current version of D.0 to version F6 and adopt an updated standard for Medicaid Subrogation.[26] The second proposed rule, if finalized, would adopt a standard for health care attachments transactions.[27] CMS also proposed a rule that, while not a HIPAA rule, is relevant to CEs. It would require payers, including CEs, to implement FHIR-based APIs for electronic prior authorization, and includes use of the HIPAA prior authorization standard.[28] Table 2 summarizes these rules.

[26] CMS, Proposed Rule, "Administrative Simplification: Modifications of Health Insurance Portability and Accountability Act of 1996 (HIPAA) National Council for Prescription Drug Programs (NCPDP) Retail Pharmacy Standards; and Adoption of Pharmacy Subrogation Standard," 87 Fed. Reg. 67634 (Nov. 9, 2022).

[27] CMS, Proposed Rule, "Administrative Simplification: Adoption of Standards for Health Care Attachments Transactions and Electronic Signatures, and Modification to Referral Certification and Authorization Transaction Standard," 87 Fed. Reg. 78438 (Dec. 21, 2022).

[28] CMS finalized this rule in January 2024, requiring, FHIR-based API standards for data exchange between providers, patients, and payers. CMS, Final Rule, "Medicare and Medicaid Programs; Patient Protection and Affordable Care Act; Advancing Interoperability and Improving Prior Authorization Processes for Medicare Advantage Organizations, Medicaid Managed Care Plans, State Medicaid Agencies, Children's Health Insurance Program (CHIP) Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans on the Federally- Facilitated Exchanges, Merit-Based Incentive Payment System (MIPS) Eligible Clinicians, and Eligible Hospitals and Critical Access Hospitals in the Medicare Promoting Interoperability Program," 89 Fed. Reg. 8758 (Feb. 8, 2024, hereafter Prior Authorization Rule).

Table 2. CMS Proposed Rules 2021-2023

Date	Promulgated Under HIPAA	Notice of Action	Purpose	Impact
November 2022	HIPAA	Noticed of Proposed Rulemaking (NPRM): Proposed Modifications to the National Council for Prescription Drug Programs Retail Pharmacy Standards and Adoption of a New Pharmacy Subrogation Standard (CMS-0056-P)	Adopt updated versions of the retail pharmacy standards for electronic transactions adopted under the Administrative Simplification subtitle of the HIPAA.	Add information to pharmacy claim to improve patient safety, differentiate quantity, refills, and break out types of costs, and increase the "dollar amount" field character length to accommodate new innovative drug therapies priced at $1 million or more.
December 2022	HIPAA	NPRM: Adoption of Standards for Health Care Attachments Transactions and Electronic Signatures, and Modification to Referral Certification and Authorization Transaction Standard (CMS-0053-P)	Adopt standards for "health care attachments" transactions and electronic signatures in conjunction with prior authorization transactions. Modify standards for the referral certification and authorization transaction.	Provide additional medical information to the claims processor that cannot be accommodated within the claim format.
December 2022 (Finalized January 2024)	Non-HIPAA (CMS)	NPRM: Interoperability and Prior Authorization	Enable the use of more current standards and API technology for the efficient exchange of data by HIPAA-regulated payers and providers.	Improve interoperable data exchange for impacted payers and providers using FHIR-based standards and implementation guides. Improve access to data for patients to support care management. Include use of FHIR-based API for purposes of prior authorization (potential impact on HIPAA prior authorization standard X12 278).

CMS also issued a Notice of Enforcement Discretion (NED) in December 2021 regarding its final rule of May 2020 on Interoperability and Patient Access. During the time the NED was in effect,

it permitted impacted payers not to implement the payer-to-payer data exchange under the rule. The action was designed to alleviate industry tension regarding implementation of payer-to-payer data exchange, avoid the risk of discordant, non-standard data flowing between payers, provide time for data standards to mature, and allow payers additional time to implement the more sophisticated payer-to-payer data exchange solutions.[29]

During the reporting period, HHS, SDOs, and industry made progress in identifying needed improvements to address predictability in standards adoption for interoperability; interoperability beyond HIPAA; and enforcement and implementation of HIPAA Standards, Code Sets, Identifiers, and Operating Rules.

Predictability in Standards Adoption for Interoperability

A streamlined standards update and rule promulgation process by CMS that produces a more nimble, transparent, and responsive approach to standards adoption would better support federal policy objectives, industry business requirements, and emerging technologies.[30] Currently, standards development, adoption, and implementation are not predictable and are not keeping pace with business and technology innovations.[31] As a result of the complexity of the standards development process, CMS has been unable to update the standards and operating rules on a regular cadence. During the reporting period, NCVHS recommended accelerating the standards review process.[32]

The current lack of predictability creates challenges for SDOs when developing and submitting standards proposals. These challenges include inadequate pre-adoption testing and lack of sufficient cost and value data to estimate the costs and efficiency gains attributable to new and updated standards. Data standardization is vital to interoperability and data exchange of both HIPAA and non-HIPAA data across the health care system. For CEs and BAs to commit to using up-to-date HIPAA standards consistently, they need to garner increased value from the standards.

---

[29] CMS, Final Rule, "Medicare and Medicaid Programs; Patient Protection and Affordable Care Act; Interoperability and Patient Access for Medicare Advantage Organization and Medicaid Managed Care Plans, State Medicaid Agencies, CHIP Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans on the Federally- Facilitated Exchanges, and Health Care Providers" 85 Fed. Reg. 25510 (May 1, 2020), and Notice of Enforcement Discretion relating to the Final Rule at 86 Fed. Reg. 70412 (Dec. 10, 2021) (notifying the public that CMS "does not expect to take action to enforce compliance with these specific provisions until we are able to address certain implementation challenges"). CMS addressed those challenges with its payer-to-payer API policies published in the final Prior Authorization Rule, released on January 17, 2024, 89 Fed. Reg. at 8975, and thus terminated the NED.

[30] Alix Goss, Chair, Subcommittee on Standards, NCVHS, "Draft Recommendations for the Predictability Roadmap," Presentation to CAQH CORE Virtual Meeting on NCVHS Predictability Roadmap Draft Recommendations, at 14 (Nov. 5, 2018).

[31] Subcommittee on Standards, NCVHS, Draft Report, "Improving Health Care System Efficiency by Accelerating the Update, Adoption, and Use of Administrative Standards and Operating Rules: A Brief History and Draft Recommendations: Paving the Way to a Predictability Roadmap" (Sept. 2018).

[32] View letter from Jacki Monson, Chair, NCVHS, to Secretary Becerra, "Recommendations to Modernize Adoption of HIPAA Transactions Standards" (July 28, 2022).

To improve interoperability, HHS and industry will need to plan and budget resources for trading partners (entities that exchange HIPAA-compliant transactions) to establish a set of criteria to evaluate and pre-test new transaction standards. Effective transaction standards must demonstrate a reasonable cost-to-value proposition.

Interoperability Beyond HIPAA

The regulatory structures established under HIPAA in the 1990s must accommodate the business needs of the 2020s. Clinical and administrative data are often commingled while new entities such as personal health apps and employer groups are using health data, often outside of the safeguards of HIPAA. Comprehensive understanding of standards maturity, cost, workforce capacity, and industry consensus and readiness for implementing new, emergent versions of standards will help inform HHS on standards under HIPAA that accommodate new technologies as well as possible alternative standards.

Enforcement and Implementation of HIPAA Standards, Code Sets, Identifiers and Operating Rules

Enforcement is an important component of HIPAA Administrative Simplification standards adoption. Through the CMS Administrative Simplification Enforcement and Testing Tool (ASETT)[33] portal, HHS receives complaints related to transactions, code sets, operating rules, and occasionally unique identifiers. The CMS National Standards Group (NSG) has the authority to investigate these complaints and conduct compliance reviews arising out of potential violations, and, when applicable, impose a corrective action plan. NSG works with violators to develop and implement corrective action plans to achieve compliance. HHS has the authority to impose fines but to date they have only required corrective action plans with follow-up to verify that the violation is corrected. HHS enforcement activities are expected to increase as the cadence of standards updates increases.

Figure 1 shows the number of valid complaints related to HIPAA administrative simplification submitted to CMS in 2023. CMS categorized most of the submitted complaints in 2023 (71%) as "invalid" because they related to issues of quality-of-care or the usability of these standards, neither of which is enforceable under HIPAA. However, NSG identified the remaining 29% of 2023 complaints as enforceable under HIPAA. Some providers have been reluctant to lodge complaints where they would be appropriate,[34] suggesting possible under-reporting. However, although low in volume, each complaint represents many transactions exchanged between and among stakeholders and is therefore significant. Additional resources to enhance the NSG compliance program with proactive auditing would put less reliance on complaint-driven intervention and emphasize industry-wide use of the HIPAA standards. The use of HIPAA named

[33] CMS provides information about ASETT on the home page of the ASETT program. ASETT provides technical guidance and a testing tool that supports non-compliance complaint submissions (with an option for anonymity) and validation of code sets to identify and resolve errors.

[34] For example., letter from Anders Gilberg, Senior Vice President, Government Affairs, Medical Group Management Association to Kathleen Cantwell, Director, Office of Strategic Operations and Regulatory Affairs, CMS, Document Identifier CMS-10148 (May 23, 2018).

standards in non-compliant ways by CEs and BAs increases the implementation time and resource costs for their trading partners.

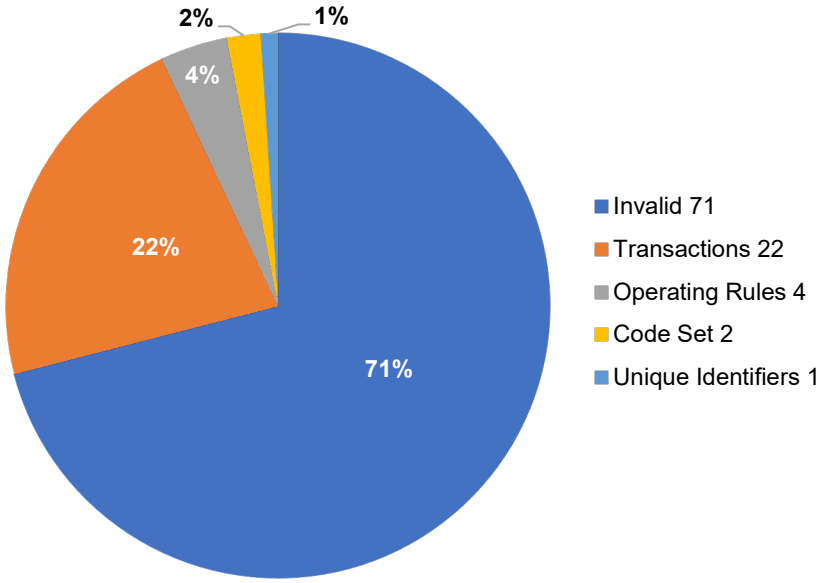

Figure 1. Complaints Received by Complaint Type 2023,
Centers for Medicare & Medicaid Services, National Standards Group, ASETT

B. Privacy, Security, and Breach Notification 2021-2023

Health information systems are dynamic, and their rate of change is outpacing existing legal and privacy frameworks. PHI is increasingly shared with non-covered entities and, therefore, moves outside of the confines of HIPAA's regulatory regime. The expansion of entities involved in health care requires new approaches to privacy and security. Appropriate use and exchange of health data, which permits timely access to and integration of patient data with other health system data, could advance research, enhance medical care, improve outcomes, and eventually save lives. However, large-scale data aggregation and exchange of these data requires a multi-faceted approach (technical, legal, educational) to control risks. As personal devices generating health information become more mainstream and may be used to train AI systems, information that consumers expect to be protected may not be covered by HIPAA, may become subject to other laws, or may lose legal protection entirely. The expansion of commercially available information, increased threats caused by cybersecurity incidents, lack of attention to health equity, concerns regarding more significant consequences of certain disclosures post-Dobbs, and data breaches must be taken into consideration when discussing privacy and security.

Commercially Available Information

The expanding availability of consumer devices that can collect and share personally identifiable information (PII), including sensitive health information, and the large and growing volume of commercially available information means that more health data will be used and disclosed outside of the protections of HIPAA. Some states and the Federal Trade Commission (FTC) are responding to this change by expanding activities to protect non-HIPAA data. The FTC and HHS

may need to coordinate on emerging issues including access to PHI, the use of location data, use of commercially available information by agencies and the public, AI transparency, and algorithmic fairness.

Cybersecurity

Cybersecurity incidents affecting hospitals and health systems have led to extended care disruptions, patient diversions to other facilities, and delayed medical procedures, putting patient safety at risk. Minimal cybersecurity hygiene requirements are needed. These requirements include hiring qualified information security employees, use of multi-factor authentication, ensuring offline backups, and disclosure of impacts and vulnerabilities to protect patient care. Adoption of NCVHS' recent recommendations on cybersecurity would significantly reduce cyberattacks.[35] Additionally, outreach, education, and technical assistance to less resourced entities following the model of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency's (CISA) Interoperable Communications Technical Assistance Program (ICTAP) would assist industry in reducing cyber threats.[36]

Health Equity

Public health, administrative, and community-level data are critical to improving the health of all Americans and addressing health inequities. State, local, territorial, and tribal entities all need timely access to public health data to carry out essential public health functions. For example, American Indian and Alaska Native communities do not always gain access to critical health data. This lack of access was especially true during the COVID-19 pandemic, resulting in poor health outcomes and excess deaths. Innovative methods and approaches to collect, use, protect, and share data responsibly during a pandemic or long-term nationwide Public Health Emergency would improve timeliness and availability of actionable health information. The new methods would focus on accessibility and timeliness of high-quality health and SDOH data, while still preserving privacy and security, to improve health equity. The continued lack of coordination and failure to address privacy and security challenges to data sharing for public health purposes will disproportionately harm historically underserved and vulnerable populations and risk the health of the U.S. population more generally.

Data Breaches

OCR reported that increases in health data breaches are largely due to BAs and other third parties.[37] The adoption of mandatory minimum cybersecurity hygiene requirements by BAs and other third parties such as hiring of qualified information security employees, use of multi-factor authentication, offline backups, risk analysis, and transparency around impact and vulnerability

---

[35] Security Rule Letter and Cybersecurity Letter, op. cit. at fn16.

[36] CISA ICTAP serves all 56 states and territories and provides direct support to state, local, tribal, and territorial (SLTT) emergency responders and government officials through the development and delivery of training, tools, and onsite assistance to advance public safety interoperable communications capabilities. More information about this program is available at SAFECOM.

[37] Timothy Noonan, Deputy Director for Health Information Privacy, Data, and Cybersecurity, OCR, "HIPAA Update from the Office for Civil Rights," presentation to NCVHS Full Committee Meeting of April 12, 2024..

disclosures would significantly reduce the risk of breaches. Continued non-compliance with existing HIPAA security requirements, particularly risk analysis, and adoption of appropriate mitigation strategies will invite increased intrusions, exfiltration of sensitive medical data, loss of trust in the health system, and opportunities for adversaries to take advantage of U.S. vulnerabilities.

HIPAA privacy provisions and IT investment incentives in the Health Information Technology for Economic and Clinical Health Act[38] (HITECH) have resulted in improvements to data privacy and security. However, new privacy and security vulnerabilities are arising because of the expansion of emerging technologies such as AI and telehealth, the lack of guidance on accounting of disclosures, and HHS' re-interpretation of provisions on maximum civil monetary penalties in 2019.[39]

HHS publishes a summary of all breaches of unsecured PHI affecting 500 or more individuals reported by CEs on a public website in accordance with the requirements in the HITECH Act.[40] Figure 2 shows the percentage of large breaches reported to OCR between September 2009 and December 2023[41] by cause of the breach. Hacking and IT incidents continue to be the leading type of breaches affecting HIPAA CEs and their BAs, followed by unauthorized access or disclosure. As many companies outsource their data processing and storage to outside parties, there are more third-party data breaches caused by software vulnerabilities, which makes it incumbent upon both the organizations outsourcing the data and the companies that host data to properly protect the data.

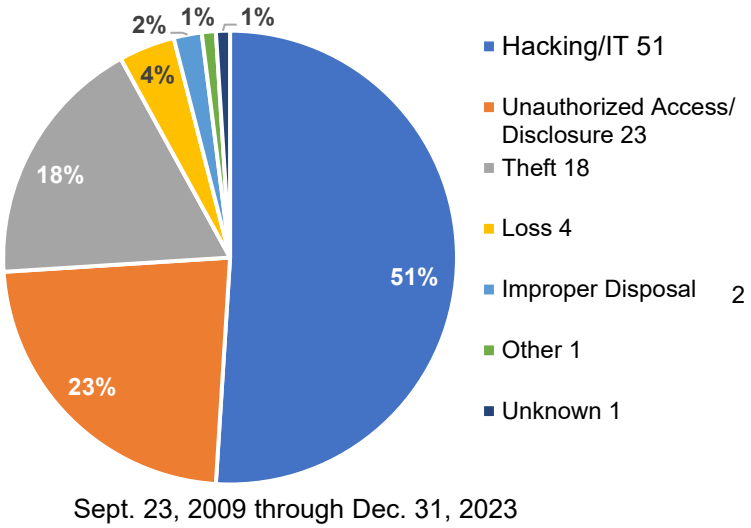

Figure 2. 500+ Breaches by Cause of Breach,
U.S. Department of Health and Human Services, Office for Civil Rights, 2022

[38] Title XIII of the American Recovery and Reinvestment Act, Public Law 111-5, 123 Stat. 226 (2009).
[39] OCR, "Notification of Enforcement Discretion Regarding HIPAA Civil Money Penalties," 84 Fed. Reg. 18151 (April 30, 2019).
[40] HITECH Act § 13402(e), codified at 42 U.S.C. 17932. The posted notices of breaches affecting 500 or more individuals may be viewed and searched on OCR's website.
[41] Noonan, *infra*, April 12, 2024

Data breaches have steadily increased over the years 2018-2023 (Figure 3), with reported large breaches nearly doubling between 2018 and 2023. The number of individuals affected by these large breaches reached almost 135 million in 2023, an approximate nine-fold increase from 2018.[42]

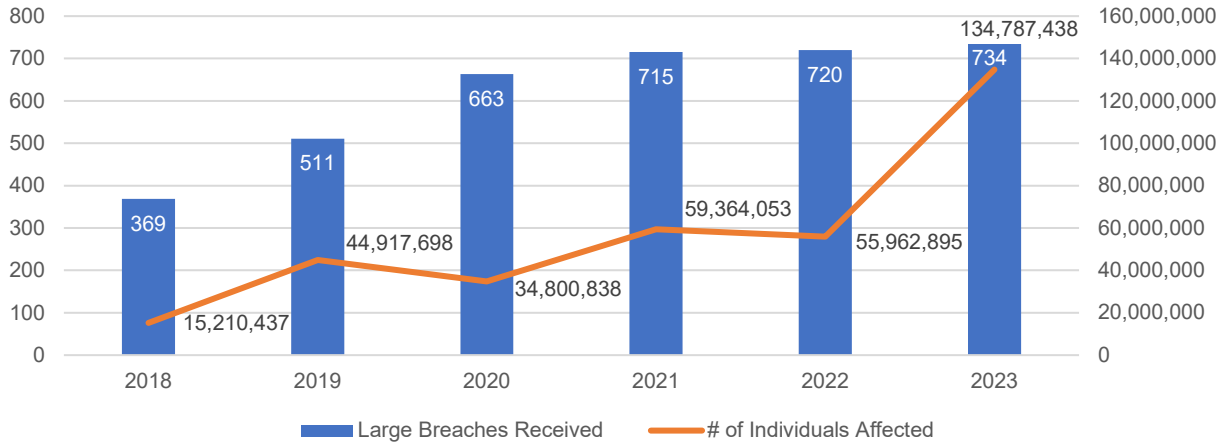

Figure 3. Large Breaches Received and # of Individuals Affected, 2018-2023, U.S. Department of Health, Office for Civil Rights

OCR investigations in 2022 uncovered elements of health data security that need improvement. The HIPAA Security Rule requires that regulated entities implement policies and procedures to prevent, detect, contain, and correct security violations and that they implement sufficient security measures to reduce risks and vulnerabilities to a reasonable and appropriate level. OCR's investigations continue to identify noncompliance with these requirements including failures to implement security measures, such as risk analysis and risk management, leaving regulated entities vulnerable to breaches of unsecured electronic PHI as cybersecurity attacks increase. Table 3 shows examples of the largest breaches reported to OCR in 2023 and are largely associated with BAs.[43]

Table 3. Largest Breaches 2021-2023, HHS/OCR

State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
TN	Business Associate	11270000	7/31/2023	Hacking/IT Incident	Other
VA	Business Associate	9179226	8/4/2023	Hacking/IT Incident	Network Server
NV	Business Associate	8952212	11/3/2023	Hacking/IT Incident	Network Server
GA	Business Associate	8861076	5/26/2023	Hacking/IT Incident	Network Server

[42] *Id.*
[43] OCR Breach Portal, *op. cit.* at fn 49.

State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
CO	Business Associate	8493379	11/6/2023	Hacking/IT Incident	Network Server
KY	Health Care Provider	5815591	5/12/2023	Hacking/IT Incident	Network Server
NJ	Business Associate	4656293	12/21/2023	Hacking/IT Incident	Network Server
FL	Business Associate	4212823	2/10/2023	Hacking/IT Incident	Network Server
FL	Business Associate	4142440	5/24/2021	Hacking/IT Incident	Network Server
WI	Business Associate	4112892	7/27/2022	Hacking/IT Incident	Network Server

Lax security practices in health care organizations make valuable health information vulnerable. An increase in cyber criminals and organized crime remotely launching ransomware attacks against U.S. hospitals, medical research laboratories, and other critical infrastructure are direct threats to public health and safety.[44] NCVHS recommended that HHS prioritize assistance to less resourced entities that may be vulnerable to cyber threats that result in breaches.[45] Evaluation of the level of compliance with the HIPAA Security Rule could allow for the provision of assistance to health care entities with the greatest need in meeting the enhanced minimum-security requirements.

III. EMERGING TRENDS AND CHALLENGES FOR CONGRESS AND OTHER LEADERS TO CONSIDER 2024-2025

As health care delivery evolves and Health IT and data sources are redefined and repurposed, Congressional and HHS efforts to standardize electronic health care administrative transactions and safeguard patients' sensitive medical information should consider addressing the demands and dependencies of a digital health care ecosystem. This section discusses trends and challenges related to standardization for interoperability, cybersecurity, and Health IT and digital innovations.

[44] Congressional Research Service, "The Change Healthcare Cyberattack and Response Considerations for Policymakers" (March 14, 2024); John Riggi, "Ransomware Attacks on Hospitals Have Changed," American Hospital Association (2020).
[45] Security Rule Letter and Cybersecurity Letter, *op. cit.* at fn 16.

A. Standardization for Interoperability

The right care at the right time by the right provider to the right patient at the right location[46] has an added a new "right"—using the right modality. Digital health care, which includes in-person, virtual, and hybrid care, depends on timely, reliable, accurate, private, and accessible data. The data, which are valuable for efficient and effective delivery and administration of care, must be transformed into actionable, understandable information that is standardized and can be disseminated securely. These data are used for clinical, public, and population health and to support state, territorial, tribal, and local government, research, and administrative systems.

The health care industry needs a comprehensive, well integrated set of standards that support health information interoperability, data privacy, and security. Harmonization of standards and data across SDOs, users, and state and federal regulatory agencies will be necessary to achieve comprehensive interoperability.

Despite progress, challenges remain to modernizing the HIPAA standards and standards process to keep pace with technological and burgeoning information needs. Updates to HIPAA standards and operating rules have not been made on a regular cadence, either because updated standards have not been put forward by the SDOs or because of regulatory process time. The United States needs a consensus framework, criteria, and method for estimating the cost and value of proposed standards to expedite future standards reviews and regulatory actions. NSG enforcement of transaction standards adoption across industry and trading partners is important to avoid proprietary solutions and costly "work-arounds" caused by non-compliance.[47]

The WHO adopted ICD-11 in 2019. The 64 member countries are currently in different stages of implementing this standard. It is important to avoid a U.S.-specific clinical modification as occurred for ICD-10, pre-adoption research, planning, and stakeholder outreach investments would facilitate a smoother and less disruptive transition to ICD-11 than what occurred in the protracted and costly ICD-9 to ICD-10 transition.[48]

Protecting PII and public health data that are exchanged between HIPAA CEs and non-HIPAA CEs is critical. Consent and authorization mechanisms must work effectively for the exchange of health information, which is important for the individual, the health plan, and the health care provider holding the individual's health information. At the state level, momentum for new

---

[46] J. Tavares, et al., "The effect of the right care, right place, right time (R3) initiative on Medicare health service use among older affordable housing residents," Health Services Research (Feb. 2023). doi: 10.1111/1475-6773.14086.

[47] ASETT is a web-based application which enables individuals or organizations to file a HIPAA and/or ACA complaint against a HIPAA CE (which includes health care providers, health plans, and clearinghouses) for potential non-compliance with the non-Privacy/Security provisions of HIPAA, including Transactions and Code Sets, Unique Identifier, and Operating Rules provisions.

[48] On April 12, 2024, NCVHS sent recommendations to Secretary Becerra on the actions urgently needed to allow the United States to partner with WHO in the development of multinational agreements regarding ICD-11, and to participate fully as decisions are being made that may affect U.S. interests and policy options. View letter from Jacki Monson, Chair, NCVHS, to Secretary Becerra, "Urgent Need for a Central Coordinating Entity for Planning and Adopting ICD-11 in the U.S." (April 12, 2024).

comprehensive privacy legislation is at an all-time high. As of June 2023, five states have adopted new comprehensive privacy laws since 2018: California, Colorado, Connecticut, Virginia, and Utah. Four additional states—Michigan, New Jersey, Ohio, and Pennsylvania—have active comprehensive privacy bills under consideration.

Although AI presents opportunities for innovation in research, clinical diagnostics, and pharmaceutical developments, it poses potential risks. It will be challenging for HIPAA privacy and security provisions to address these risks, given that the private sector is moving faster than government and policy. The expansion of non-HIPAA health information sharing through AI and other means requires review and potential adjustments for non-HIPAA health information related to data confidentiality protection, intended and unintended use of data, informed consent and data collection and use awareness.

B. Cybersecurity

The cybersecurity threat environment is rapidly evolving and requires enhancements to prevent attacks and improvements to recovery. Health care is a major target for cyberattacks, posing risks to access and potentially impacting patients' clinical outcomes. Cyber incidents affecting hospitals and health systems have led to extended care disruptions, patient diversions to other facilities, and delayed medical procedures, all of which put consumer and provider safety at risk.[49]

Health care entities have taken steps to plan, execute, and recover from cybersecurity incidents ranging from prevention to improving their ability to mitigate damage to systems and processes, to improved cyber "hygiene" and adopting a security-centric mindset and habits that help them avoid and mitigate the damage due to breaches.[50] Entities can reduce the number and severity of cybersecurity incidents by assessing safety and security issues and solutions,[51] particularly related to the expanded operationalization of AI.

All HIPAA CEs and BAs should implement security programs in the Security Rule through a risk management approach, consistent cyber incident reporting, and implementation of security controls. Implementing privacy and security requirements for data release, in addition to HHS revisiting current data aggregation or disaggregation standards, will support the essential data needed to assess and improve population health, including that of urban and tribal members. Protections of these data may improve consumer confidence and provide "trust," which is required for the exchange of data.

---

[49] Change Healthcare, a unit of UnitedHealth Group (UHG), was impacted by a cybersecurity incident in late February 2024 that has caused major disruptions in health care and billing information systems nationwide. The incident poses a direct threat to critically needed patient care and essential operations of the health care industry.

[50] NIST, Spec. Pub. 800-160, Vol. 2, Rev. 1, "Developing Cyber-Resilient Systems: A Systems Security Engineering Approach" (Dec. 9, 2021).

[51] Basic security controls include anti-theft devices, digital forensics, network segmentation, business disaster and continuity recovery plan, multi-factor authentication, ransomware detection, vulnerability scans, penetration testing, and information sharing.

The expanded need and use of emerging technology in health care, particularly AI, has created additional complexity for different facets of interoperability across the industry. Any AI health care strategy used by HIPAA CEs will likely demand and be dependent on a data strategy that provides accurate and timely information and the foundation for descriptive, diagnostic, predictive, and prescription analytics based on data from across the digital infrastructure. HIPAA CEs will need AI to help them defend against vulnerabilities related to new data sources and workforce challenges, such as lack of situational awareness and specialized skills, or the need for more ongoing training AI might also assist HIPAA CEs in knowing the data content included in the source data used for algorithms and the location of these source data, which can support a robust security program.

AI can also be a mechanism for addressing privacy concerns. Defensive AI uses self-learning algorithms to defend against threats. Future generations of Privacy Preserving Machine Learning in health care may enable trustworthy defensive systems through an integrated and supportive process, changes in behaviors, and innovative practices.

C. Medical Privacy Disclosure Risks Post-Dobbs

The Supreme Court's decision in Dobbs resulted in some states reactivating or enacting laws that reduce access to the full range of necessary reproductive health care treatments. As a result, PHI may be disclosed in ways that cause harm to the interests that HIPAA seeks to protect. This risk of disclosure likely increases the potential to undermine access to and the quality of health care. New and reenacted state laws have introduced uncertainty and burden across HIPAA CEs and have unintended consequences for public health activities. There is a risk that without the confidence that the privacy of patient records assures, patients may forego necessary care, leading to decreases in health outcomes and risks to patient safety. There is already evidence of providers failing to properly document care in their records, physicians moving away from states where the full range of necessary reproductive care is not legal, and medical students avoiding medical schools or advanced training in states where the full range of necessary care is not legal. These factors will cause risks to patients and liability for providers, and will decrease the availability and quality of care in areas of the country that are already disadvantaged.

NCVHS submitted comments on the NPRM that would amend the HIPAA Privacy Rule to support reproductive health care privacy.[52] HIPAA CEs have an opportunity and obligation to review deidentification and disclosure practices and procedures, including those associated with data exchanged through Health Information Exchanges, to protect sensitive health information. This is especially so as some states seek to interfere in deeply personal medical decisions by criminalizing activities to seek, obtain, provide, or facilitate necessary reproductive care, or penalize patients, health care providers, and others who engage in those activities.

[52] View Letter from Jacki Monson, Chair, NCVHS, to Secretary Becerra, "Comments on Docket #HHS-OCR-2023-0006 Notice of Proposed Rulemaking, 'HIPAA Privacy Rule to Support Reproductive Health Care Privacy'," (June 14, 2023, hereafter NCVHS Reproductive Health Comments).

D. Transition to ICD-11

WHO adopted ICD-11[53] in 2019 and made it available for use globally as of January 1, 2022. ICD classifications are used primarily for mortality reporting, morbidity documentation, and health research purposes. The revised taxonomy has the potential for a more expansive view of patient health and leverages existing digital capabilities. ICD-11 has new characteristics that could be advantageous for morbidity reporting. It is designed to be continuously and seamlessly updated, with greater ease of coordination with other classifications and terminologies such as Systemized Nomenclature of Medicine–Clinical Terms (SNOMED CT). ICD-11 is also designed to capture data related to social risk, and social and community health factors, to inform research and interventions in support of health equity and overall better health.

The United States' transition from ICD-9 to ICD-10 incurred many costs and resource burdens and was completed much later than the other WHO member countries. If the United States is to avoid repeating this scenario in the adoption of ICD-11, centralized coordination and leadership is essential. Centralized coordination would reduce burden arising from online automation, usher in improvements in international comparability in reporting and research, and permit implementation of ICD-11 taxonomy into modern systems and standards. Research to understand the value of ICD-11 for U.S. applications and actions to avoid a proprietary or U.S.-specific clinical modification would be preferable to the situation that occurred for ICD-10.[54] Delayed implementation of ICD-11 could result in challenges to funding for benefit/cost analysis, education, outreach, and federal infrastructure; health information systems implementations; integration with other health care coding, classification, and terminology systems; communication and stakeholder engagement; and workforce training requirements.[55]

In 2022, NCVHS established a Workgroup on Timely and Strategic Action to Inform ICD-11 Policy (ICD-11 Workgroup) to gather information from a broad range of sources to develop advice and recommendations for HHS regarding adoption of ICD-11 as a regulatory code set.

E. Health IT and Digital Innovations, including AI

As some transaction standards approach full adoption, efforts should focus on transactions with high savings opportunities, such as eligibility and benefit verifications and claim submissions. Understanding and addressing issues that providers and payers face when automating

[53] ICD is the global standard for health data, clinical documentation, and statistical aggregation. It provides a common language for recording, reporting, and monitoring diseases, enabling the world to compare and share data in a consistent and standard way—among hospitals, regions, and countries, and over periods of time. It facilitates the collection and storage of data for analysis and evidence-based decision-making by enabling systematic recording, reporting, analysis, interpretation, and comparison of mortality and morbidity data.

[54] WHO Fact Sheet: ICD–11 is a flexible system that eliminates the need for local variants and enables documentation of all kind of clinical detail. In such a way, and in combination with the simplified coding, it can be integrated seamlessly in the routine of clinical documentation.

[55] View letter from Nick Coussoule, Chair, NCVHS, to Secretary Becerra, "Updated Recommendations for Immediate Action on ICD-11" (Sept. 10, 2021).

workflows is necessary as new opportunities and challenges arise, including AI related to the optimization of emerging technologies.

The rapid advancement of digital technologies has led to transformative changes across various industries due to the increased volume of data (i.e., standard data exchange, sensors, and user interactions). AI plays a pivotal role in this digital transformation, particularly through the use of algorithms, which process and analyze these data to extract meaningful insights. These insights inform decision-making processes across organizations.

AI algorithms inherit any biases that may already be present in the data on which they are trained. Biased outcomes may mean that some populations may be disproportionately negatively affected, and therefore, the use of AI could perpetuate existing inequalities. To address potential algorithmic bias or limitations in the data, it is essential to understand both the algorithm itself and the data it relies on, including its source. This understanding is crucial for consideration of how to mitigate any gaps in critical data. Data sources that have not historically been included in health care data analysis, such as those used for SDOH, include both unstructured and structured data, creating another complexity that is both beneficial and presents potential implementation and operational risks.

As with all digital transformation, a roadmap, developed in collaboration with federal, state, and industry stakeholders, is necessary for successful implementation. With emerging technologies and the reliance on data to fuel automation and support health care delivery and decisions, information about the data used and the shortcomings of software should be transparent to permit harmonization of information while minimizing misinformation. The lack of incentives for health care entities to adopt data standards leads to variation in data collection across the health care system resulting in persistent data gaps and disparities in outcomes. The development and implementation of the roadmap ideally would include an integrated and supportive process, change in stakeholder behaviors, and inclusion of innovative practices. The United States should address challenges to optimal use of AI, such as the availability of workforce talent, scalability, ethical and legal factors, algorithmic bias or universe limitations, workflow challenges, and clarity on the type(s) of AI being considered.

F. Quantum Readiness

Preparations for the introduction of quantum resistant cryptographic methods have been under way for over 2 years,[56] and the National Institute of Standards and Technology is expected to publish final standards for algorithms that can resist attack by quantum computers in 2024.[57] A roadmap of guidance for organizations to help explain, for example, how to determine which data required update security protections, would be helpful.

There is a Health IT and digital innovations divide, meaning inequitable access to new technologies including broadband Internet, FHIR APIs, AI solutions, and others. The inequities exist across rural, small, and mid-sized health care practices, community health centers, historically underserved persons or populations, and public entities that are lesser resourced

[56] William Barker, et al., NIST, "Project Description: Migration to Post-Quantum Cryptography" (Aug. 2021).
[57] NIST, Press Release, "NIST to Standardize Encryption Algorithms That Can Resist Attack by Quantum Computers" (Aug. 24, 2023).

than their better resourced counterparts. Closing this divide requires a data and Health IT strategy that addresses barriers that lesser resourced entities encounter. These entities often struggle to comply with regulations and other requirements due to workforce limitations, poor broadband connectivity, and other resource limitations.

In summary, NCVHS has diligently worked to advance administrative simplification of HIPAA and related regulations and privacy and security provisions and guidance. During the 2021-2023 reporting period, NCVHS focused on standardizing electronic health care administrative transactions, safeguarding patients' sensitive health information, and addressing emerging trends. As NCVHS looks ahead to 2024-2025, it recommends prioritizing standardization for interoperability, enhancing cybersecurity measures, and monitoring emerging technologies to support innovation while maintaining necessary safeguards.

Appendix A: Summary of NCVHS Recommendations to DHHS by the Standards Subcommittee and ICD-11 Workgroup

Date	Main Topic or Theme of the Report and Date of Hearing	Summary of NCVS Recommendations to DHHS
June 2023	Response to May 2022 request from CAQH CORE to recommend adoption of updated and new operating rules	Recommendations informed by November 2022 Request for Comments and January 2023 Listening Session on adoption of updated and new Operating Rules, approving some proposed rules, delaying adoption of attachment and prior authorization until final rule enacted.
June 2023	Response to June 2022 request from X12 to recommend adoption of updated version of standard for Claims and Electronic Remittance Advice Transactions to Version 008020	Recommends no adoption of 00820 and cites need for more information on the new standard's compatibility across years and industry and requests more detailed information on value proposition (cost/value) of new standards.
July 2022	Modernize Adoption of HIPAA Transaction Standards Based on NCVHS sponsored listening Session held 6/9/22 to address new drivers of transformation in healthcare data exchange & convergence of clinical and administrative standards (ONC HITAC and ICAD Task Force)	Informed by industry input, recommendations designed to support the transformative changes occurring in health care delivery systems, payment methodologies, standards development, and rule adoption.
March 2022	Modernize HIPAA and other Health IT standards to improve care and reduce Burden	Recommends a new, broader framework that will converge the HIPAA administrative simplification standards with clinical, public health (PH) systems, and other wellness data standards, such as for SDOH and sexual orientation and gender identity data and calls for updates to HIPAA and related standards and a streamline standards process.
September 2021	Updated Recommendations for Immediate Action on ICD-11	Updated recommendations for HHS to commence ICD-11 research and strategic communications and outreach to avert significant avoidable transition cost and burden to the U.S. health care system, including PH, like those experienced in the recent transition from ICD-9 to ICD-10.

Appendix B: Letters of Recommendations Submitted to DHHS by the Privacy & Security Subcommittee

Date	Main Topic or Theme of the Report	Summary of NCVHS letter(s) or relevant reports
November 2023	Letter to the Secretary on Recommendations to Strengthen the HIPAA Security Rule	Require implementation of security programs in the Security Rule by HIPAA CEs and BAs that include: • Implementation of a risk management approach • Establishment of consistent cyber incident reporting • Reduction in ambiguous, optional, and addressable security controls • Implementation of HIPAA security rules in AI systems
June 2023	Comments on Docket # HHS-OCR-2023-0006, Notice of Proposed Rulemaking, "HIPAA Privacy Rule to Support Reproductive Health Care Privacy	To reduce the likelihood of health records being employed to harm patients or others for seeking, obtaining, providing, or facilitating health care, NCVHS recommends that HHS: • Distinguish between legal v. illegal care • Prohibit disclosures for criminal, administrative, investigative actions connected with seeking medical care • Redefine reproductive health care • Require attestations for PHI requests • Include a Notice of Privacy Practices in plain, clear language • Address the rule in relation to telehealth, telemedicine, medical devices, apps, wearables, interoperability, information blocking, and the Cures Act TEFCA
January 2023	Ongoing and Emerging Issues in Privacy and Security in a Post COVID-19 Era: An Environmental Scan A report for the National Committee on Vital and Health Statistics	Ongoing and Emerging Issues in Privacy and Security in a Post COVID-19 Era: An Environmental Scan includes the following: • Emerging state and federal health privacy laws • Deidentification • Law enforcement access to PHI and review exemptions • AI and machine learning standards and transparency • FTC-HHS coordination and joint guidance on Commercial Surveillance and Data Security

Date	Main Topic or Theme of the Report	Summary of NCVHS letter(s) or relevant reports
December 2022	Letter to the Secretary on Recommendations regarding Privacy, Confidentiality, and Security Considerations for Data Collection and Use During a PHE	Develop a national governance strategy specific to PHEs in collaboration with federal, tribal, state, territorial, and local partners that increases trustworthiness in data collectors, data stewards, and those who share the data collected in and after the PHE, addressing inequities in the collection and timely reporting of datapoints on disaggregated race, ethnicity, geography, and age
December 2022	Letter to the Secretary on Recommendations for HHS, States and Territorial PH Authorities to Improve PH Data Sharing with Tribal Epidemiology Centers (TECs) and Other Designated Tribal PH Authorities (ODTPHAs)	Specific recommendations for HHS actions to improve the timely access to PH data for Tribal Epidemiology Centers (TECs) and Other Designated Tribal PH Authorities (ODTPHAs) from federal, state, and local PH authorities and health care providers, reducing barriers to data access by TECs and ODTPHAs that contributed to delays in responding to the COVID-19 PHE
May 2022	Letter to the Secretary on Recommendations to Strengthen Cybersecurity in Healthcare	In response to the rising number of cybersecurity incidents affecting the health care industry, recommendations include: Strengthening the HIPAA Security Rule by 1.A. Require CEs to implement the specification in the Security Rule or to adopt a documented reasonable alternative 1.B. Include additional minimum cybersecurity hygiene requirements 2. Mandate basic cybersecurity requirements for any organization that is a recipient of federal funds 3. Further enhance communication and education regarding the HIPAA Security Rule and security threats and incidents by: 3.A. Providing more guidance on risk analysis requirements 3.B. Facilitating, with other appropriate government agencies, the coordination and identification of threats to critical infrastructure 3.C. Leveraging, cybersecurity newsletters as real-time playbooks on common cybersecurity incidents

Appendix C: NCVHS Membership Roster

For biographical information of Committee members, please visit the NCVHS website: https://ncvhs.hhs.gov/membership/full-committee/.

CHAIR

Jacki Monson, JD
Senior Vice President, Chief Integration Officer
Sutter Health
Sacramento, CA

MEMBERSHIP

Angela M. Alton, MPA
Vice President and Chief Privacy Officer
City of Hope
Chicago, IL 60610

Tammy Feenstra Banks, MBA, FACMPE
Principal/Consultant ImpactQue, LLC
Gobles, MI

Denise Chrysler, JD
Director, Mid-States Region
Network for Public Health Law
University of Michigan School of Public Health
Ann Arbor, MI

Catherine Molchan Donald, MBA
CFO and Director of General Operations
Alabama Department of Public Health
Montgomery, AL

Jamie A. Ferguson
VP, Health IT Strategy & Policy
Kaiser Permanente
Anacortes, WA

Michael L. Hodgkins, MD, MPH
Healthcare Consultant
San Diego, CA

R. Lenel James, MBA
Business Lead
Health Information Exchange & Innovation
Blue Cross Blue Shield Association
Tinley Park, IL

Debra Strickland, MS
Technical Project Manager
Conduent
Wallingford, CT

Steven Wagner, MBA
Health Information Enterprise Architect (Retired)
Fort Mohave, AZ

Valerie J.M. Watzlaf, PhD, MPH, RHIA, FAHIMA
Vice Chair of Education and Associate Professor
University of Pittsburgh
Department of Health Information Management
School of Health and Rehabilitation Science
Pittsburgh, PA

Wu Xu, PhD
Adjunct Faculty
Sociology, Bio-Medical Informatics, and Clinical Epidemiology
University of Utah
Salt Lake City, UT

Appendix D: Acronyms Used in This Report

ACA	Patient Protection and Affordable Care Act
AI	artificial intelligence
API	Application Programming Interface
ASETT	Administrative Simplification Enforcement and Testing Tool
BA	business associate
CE	covered entity
C.F.R.	Code of Federal Regulations
CISA	Cybersecurity and Infrastructure Security Agency
CMS	Centers for Medicare & Medicaid Services
CORE	Committee on Operating Rules for Information Exchange
EFT	electronic fund transfer
EHR	electronic health record
FHIR	Fast Healthcare Interoperability Resources®
FTC	Federal Trade Commission
HHS	U.S. Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health Act
HL7	Health Level Seven International®
ICD	International Classification of Diseases
ICTAP	Interoperable Communications Technical Assistance Program
IT	information technology
NCPDP	National Council for Prescription Drug Programs
NCVHS	National Center for Vital and Health Statistics
NED	Notice of Enforcement Discretion
NPRM	Notice of Proposed Rulemaking
NSG	National Standards Group
OCR	Office for Civil Rights
ODTPHA	Other Designated Tribal PH Authorities
ONC	Office of the National Coordinator for Health Information Technology
PHE	Public Health Emergency
PH	public health
PHI	protected health information
PII	personally identifiable information
SDO	Standards Development Organization
SDOH	social determinants of health
TEC	Tribal Epidemiology Center
TEFCA	Trusted Exchange Framework and Common Agreement
U.S.C.	United States Code
USCDI	United States Core Data for Interoperability
WHO	World Health Organization