American College of Emergency Physicians®
ADVANCING EMERGENCY CARE

April 7, 2025

The Honorable Brett Guthrie
Chairman
Committee on Energy and Commerce
U.S. House of Representatives
Washington, D.C. 20515

The Honorable John Joyce, M.D.
Vice Chair
Committee on Energy and Commerce
U.S. House of Representatives
Washington, D.C. 20515

Dear Chairman Guthrie and Vice Chair Joyce:

On behalf of the American College of Emergency Physicians (ACEP) and our nearly 40,000 members, thank you for the opportunity to respond to the Energy and Commerce Committee data privacy working group's (working group) recent request for information (RFI) to help inform comprehensive federal data privacy and security standards. As you well know, ensuring the privacy and confidentiality of protected health information (PHI) for our patients is a fundamental responsibility of emergency physicians and is a key principle in ACEP's Code of Ethics for Emergency Physicians.[1]

Given the distinct nature of emergency medicine and the open setting of the (ED), guaranteeing patient privacy and confidentiality and maintaining best practices for data privacy and security present unique challenges that often prove more difficult than most other practice settings. As the working group reviews feedback and insights from a broad spectrum of stakeholders throughout the country, we appreciate the opportunity to share our experiences and thoughts on these issues from the perspective of emergency medicine.

Roles and Responsibilities

With respect to health care, a federal comprehensive data privacy and security law must take into account an exceptionally complicated health information technology (HIT) system that is not always interoperable and is also subject to more stringent state and federal regulations and laws governing privacy and security. A comprehensive law must also consider the impact of growing consolidation within health care, particularly how the size of an entity/organization and the sensitivity of the data and information they control make them uniquely attractive targets for cyberattacks. A comprehensive data privacy and security law should also consider an entity's size, as well as its responsibilities to consumers and those who work with or within those systems, its ability to secure and protect sensitive information, and what processes are in place to mitigate and respond to security breaches or other adverse events to prevent disruptions in the delivery of care. Consider the recent cyberattack on Change Healthcare, a UnitedHealth Group (UHG) subsidiary and the nation's largest medical claims processor. As a result of the largest health care data breach

[1] ACEP Policy Statement, "Code of Ethics for Emergency Physicians," revised October 2023, https://www.acep.org/siteassets/new-pdfs/policy-statements/code-of-ethics-for-emergency-physicians.pdf

WASHINGTON, DC OFFICE
901 New York Ave, NW
Suite 515E
Washington DC 20001-4432

202-728-0610
800-320-0610
www.acep.org

in history, UHG's own estimates suggest that 190 million people were affected by the cyberattack, with UHG CEO Andrew Witty testifying before Congress in 2024 that one-third of all Americans were likely affected by the data breach.

The full impact was not limited to the breach of sensitive PHI – while UHG estimated the cost of the attack to be nearly $3 billion, the sheer scale of the incident caused devastating ripple effects throughout the health care system that harmed both patients and their health care providers. The breach resulted in near-total disruption to critical health care systems, harming patients who were unable to obtain life-saving medications and treatments like chemotherapy, insulin, and cancer drugs, and halting a wide variety of physician operations, including patient eligibility verification, claim submissions and payments, prior authorization procedures, electronic remittance, and others. These disruptions have had long-term and direct impacts on physician practices, especially smaller practices, who lost significant amounts of revenue and devoted already scarce resources and staff to administrative procedures in the hopes that they could simply remain afloat until normal operations resumed, with many tapping into personal savings and opening lines of credit simply to maintain operations and patient care.

This crisis not only exposed the vulnerabilities in our interconnected health IT systems but also highlighted the dangerous market dynamics that allow large entities to consolidate even further in the wake of such failures. If health care consolidation continues to accelerate, future cyberattacks could be just as or more disruptive than the Change Healthcare attack with even larger sets of sensitive data at risk. A federal privacy law must include safeguards to ensure that future disruptions are prevented with adequate oversight and answered with relief mechanisms that protect patients and health care providers and ensure accountability—especially when systemic failures can be weaponized to consolidate market power. As the working group develops policy proposals to address data privacy and security, we ask you to consider how a federal data privacy and security framework could prevent and help provide a better response to future incidents.

Personal Information, Transparency, and Consumer Rights

Appropriate Scope of a Comprehensive Law & Definitions

A federal comprehensive data privacy and security law should be structured to apply broadly to personally identifiable information (PII) while also providing distinct, heightened protections for sensitive personal information (SPI). When defining these terms, it is critical to ensure that the law aligns with existing health care privacy regulations, particularly the Health Insurance Portability and Accountability Act (HIPAA), without impeding physician ability to use and exchange necessary data for patient treatment, reimbursement, and operational purposes.

The term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual (U.S.C. § 552a(a)(5).[2] Therefore, personal information should be defined as any data that can be used to identify an individual, or be reasonably linked to an individual. This would include, but is not limited to, names, phone numbers, email addresses, physical addresses, Social Security numbers, demographic information, and online

[2] https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition/definitions#individual

identifiers such as IP addresses or device IDs. Given the health care sector's increasing reliance on digital platforms and growing implementation of augmented or artificial intelligence (AI) tools, this definition should also account for emerging forms of identification, including behavioral biometrics and location-based data, as well as others as identified by stakeholders and experts within these fields.

Additionally, ACEP recognizes that sensitive personal information should be considered a separate informational subset requiring enhanced safeguards to prevent potential harm stemming from misuse or improper disclosure. In the health care sector specifically, clinicians often work with protected health information (PHI) as defined under HIPAA, which encompasses medical histories, treatment records, laboratory test results, imaging scans, and physician notes. Specifically, "individually identifiable health information" is information, including demographic data, that relates to:

- the individual's past, present or future physical or mental health or condition;
- the provision of health care to the individual;
- the past, present, or future payment for the provision of health care to the individual; and,
- that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual." [3]

Additionally, genetic data, biometric information, mental health records, and substance use disorder treatment records should be included in the definition of sensitive personal information (SPI) due to their deeply personal nature and potential for misuse. However, it is important to acknowledge that the current ED boarding crisis creates unique and unintended privacy challenges. Due to extreme overcrowding, patients are often evaluated or treated in hallways or other non-private areas in the ED and may be forced to inadvertently disclose sensitive personal information in close proximity to others. In these chaotic and overburdened environments, it becomes increasingly difficult to safeguard confidentiality, despite the best efforts of clinical staff. A federal privacy law must recognize these real-world constraints and avoid imposing requirements that are impractical or unworkable in emergency settings already operating under tremendous strain.

The scope of a federal privacy law must recognize the distinct nature of health data and ensure that its protection does not inadvertently interfere with the ability of physicians and health care providers to deliver timely, effective, and coordinated care. Protecting patient privacy is paramount; however, health data must also remain accessible for emergency treatment, public health reporting, and quality improvement efforts. Any regulations governing the collection, processing, and transfer of SPI must be designed to facilitate, rather than hinder, interoperability between health systems.

When addressing the scope of the law, Congress should work to ensure that federal law does not result in fragmentation or inconsistency in the way health data is handled. For instance, ACEP has previously expressed concerns about proposals that allow patients to selectively restrict portions of their medical records from being shared.[4] While patients should have control over their health data, allowing for ad hoc restrictions on information sharing could severely compromise interoperability, introduce inconsistencies, and create miscommunications in care.

---

[3] https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html - :~:text=Information is Protected-,Protected Health Information.,health information (PHI)."

[4] ACEP Response to Reps. DeGette & Bucshon Request for Information on Impact of 21st Century Cures Act, August 2024, https://www.acep.org/siteassets/new-pdfs/advocacy/acep-response---cures-rfi.pdf

ACEP believes that it is important to establish a foundation of standards to build interoperable electronic health information (EHI) that supports patient care across health systems and supports the idea of a common data framework specifically for quality measurement by centering the data elements that are crucial for measure development. Increased interoperability and ease of quality measurement will reduce administrative burden on emergency physicians and other health care professionals, allowing delivery of the highest quality of patient care to remain our focus. Barriers to interoperability can introduce unnecessary administrative burdens for health care providers that delay care provided. For example, if different electronic health record (EHR) platforms implement varying restrictions on data access, the ability of emergency physicians to obtain complete and accurate patient histories may be significantly impaired and could create instances of unnecessary duplicative screening, ultimately jeopardizing patient safety, and reducing the quality of care.

Disclosures re: Collection, Processing, and Transfer of Personal Information and Sensitive Personal Information

Consumers should be informed about when and under what circumstances their data may be shared with external entities, and, where applicable, they should be given the opportunity to opt out of certain types of data transfers, provided that such restrictions do not interfere with essential medical care. As ACEP has previously noted in response to regulatory proposals regarding information blocking and data segmentation, it is important to ensure that consumer rights are structured in a way that does not compromise the accuracy, completeness, and interoperability of medical records. Allowing for the selective redaction or segmentation of medical data, without a standardized mechanism for implementing such restrictions across EHRs, could lead to serious clinical consequences, including delays in diagnosis and treatment, increased administrative burden on providers, and potential safety risks for patients.

Accounting for Existing Federal & State Sectoral Laws (e.g., HIPAA)

A federal comprehensive privacy law must align with existing privacy frameworks, particularly those governing health care, financial data, and consumer protections. Sector-specific laws, such as HIPAA in the health care space, have established longstanding protections for sensitive information, and any new legislation must harmonize with these frameworks rather than introduce conflicting requirements that could burden health care providers or impede patient care.

HIPAA has long served as the foundational framework for safeguarding PHI in the United States. It ensures that patient data remains accessible for treatment, while maintaining appropriate privacy and security standards. ACEP has expressed concerns that some recent privacy proposals—especially those that allow for overly broad patient control of record segmentation— hinder interoperability, undermine continuity of care, and create confusion and risk in emergency settings. Emergency physicians depend on complete, accurate, and timely information to make life-saving decisions. Policies that allow fragmented data access, if not carefully aligned with HIPAA, could result in medical errors or delays in care. A new federal privacy law should preserve the flexibility that HIPAA provides for information sharing in treatment, payment, and health care operations.

In addition, the growing patchwork of state privacy laws creates compliance challenges and leads to fragmentation of protections for patients across state lines. Congress should work to ensure that federal law guarantees seamless interoperability and avoids a regulatory landscape that imposes different data rights and obligations depending on geography. A uniform federal standard can ensure

consistency for consumers and reduce the operational and legal complexity for providers who deliver care across multiple states.

In summary, a federal privacy law should:

- Protect patient privacy and confidentiality;
- Ensure that regulations enhance, not inhibit, secure data sharing and interoperability to facilitate high-quality and timely care;
- Recognize the real-world impact of infrastructure failures, require proactive planning and robust security measures to protect sensitive information and PHI, and accountability for breaches of sensitive information and PHI.
- Preserve HIPAA's role as the governing standard for health care data; and,
- Ensure a legal and regulatory environment that does not complicate or delay care delivery and operations.

Thank you for considering our response to this important RFI. ACEP stands at the ready to help this working group develop legislation that ensures the highest standards of data privacy and security and protects access to the high-quality lifesaving emergency care our patients need and deserve.

Sincerely,

Alison J. Haddock, MD, FACEP
President, American College of Emergency Physicians