January 23, 2023

The Honorable Chuck Schumer
Majority Leader
United States Senate
Washington, DC 20510

The Honorable Kevin McCarthy
Speaker of the House
United States House of Representatives
Washington, DC 20515

The Honorable Mitch McConnell
Minority Leader
United States Senate
Washington, DC 20510

The Honorable Hakeem Jeffries
Minority Leader
United States House of Representatives
Washington, DC 20515

Dear Leader Schumer, Speaker McCarthy, Leader McConnell, and Leader Jeffries,

On behalf of the American Health Information Management Association (AHIMA), we thank you for your leadership in Congress, and we applaud your dedication to improving the country's health system.

AHIMA is a global nonprofit association of health information (HI) professionals. AHIMA represents professionals who work with health data for more than one billion patient visits each year. The AHIMA mission of empowering people to impact health drives our members and credentialed HI professionals to ensure that health information is accurate, complete, and available to patients and clinicians. Our leaders work at the intersection of healthcare, technology, and business, and are found in data integrity and information privacy job functions worldwide.

Health information is complex, nuanced, and ever-changing. An electronic signifier of identity, its integrity is as essential as a fingerprint or social security number. The data that comes with every healthcare experience – every conversation, knee tap, and blood draw – generates essential information that can significantly impact our personal and collective wellbeing. The responsible collection, protection, and analysis of health information allows providers to provide effective care, fosters innovation, encourages researchers to make life-saving discoveries, and offers individuals an opportunity to maintain good health.

As an organization representing health information professionals, we would like to outline our top priorities as Congress works to bolster and modernize the health system.

Patient Identification

One of the most pressing issues for patient safety and interoperability within the health system today is the lack of a national strategy around patient identification. Today, there is no consistent and accurate way of linking a patient to their health information as they seek care across the continuum. Countless

times every day a patient record is either mismatched or goes unmatched. Medications are prescribed, allergies are missed, and duplicate tests are ordered. Without the ability of clinicians to correctly connect a patient with their medical record, lives have been lost and medical errors have needlessly occurred. These are situations that could have been avoided had patients been able to be accurately identified and matched with their records. This problem is so dire that one of the nation's leading patient safety organizations, the ECRI Institute, named patient misidentification among the top ten threats to patient safety.[1]

The lack of a national strategy on patient identification also causes financial burdens to patients, clinicians, and healthcare institutions. The expense of repeated medical care due to duplicate records costs an average of $1,950 per patient inpatient stay, and over $1,700 per emergency department visit. Thirty-five percent of all denied claims result from inaccurate patient identification, costing the average hospital $2.5 million and the US healthcare system over $6.7 billion annually.[2] In a recent survey by the Patient ID Now coalition, 72% of respondents agreed that there are delays in billing and reimbursement due to inaccurate patient information, and 70% indicated that patients undergo or receive duplicative or unnecessary testing or services due to difficulties in managing patient identities.

The main barrier to the creation of a national strategy on patient identification is appropriations language, Section 510, that has been included in the Labor, Health and Human Services, Education, and Related Agencies (Labor-HHS) appropriations bill for more than two decades. Put in place before the Health Insurance Portability and Accountability Act (HIPAA) was fully implemented, the ban, which states that HHS is prohibited from "spending any federal dollars to promulgate or adopt a national unique patient identifier," has effectively halted HHS from taking any steps to put into place a national strategy to address patient identification.

AHIMA strongly encourages Congress to make patient identification a priority for patient safety and public health, and recommends that policy around patient identification:
- supports the repeal of Section 510 from the Labor-HHS appropriations bills within the federal budget, and supports the adoption of a nationwide patient identification strategy, and;
- supports legislative solutions that decrease error rates for patient medical records and improves standardization of data elements within patient records to advance semantic interoperability.

Social Determinants of Health

AHIMA strongly supports the use of public policy to encourage and improve the collection, access, coding, sharing, and use of social determinants of health (SDOH) to enrich clinical decision-making and improve health outcomes, public health, and health iniquities in ways that are culturally respectful. Today, there are a lack of standards to encourage the collection and use of SDOH data, and a lack of digital infrastructure and robust technical capabilities to support functional, structural, and semantic interoperability across clinical and community-based organizations and service providers. In a recent survey conducted by AHIMA, specific challenges were found relating to the collection and coding of SDOH data. Lack of structured fields in the patient's electronic health record (EHR), lack of incentives for collecting the data, organizational priorities, and the provider's availability to address the patient's social

---

[1] Top 10 Patient Safety Concerns for Healthcare Organizations, Available at:
https://www.ecri.org/EmailResources/PSRQ/Top10/2017_PSTop10_ExecutiveBrief.pdf
[2] https://www.blackbookmarketresearch.com/blog/improving-the-patient-identification-process-and-interoperability-to-decrease-patient-record-error-rates

needs issues all impacted the number and type of SDOH elements collected and coded across the health sector. As Congress works to address SDOH issues, AHIMA recommends that Congress:

- Provide financial and technical support to train providers on how best to collect, use, and share social needs information, and support for continued and expanded research on how best to collect, use, and share SDOH data, as well as the workforce skills needed to do so, and;
- Support passage of legislation, including the LINC to Address Social Needs Act, which provides funding, technical resources, and infrastructure to support coordination between healthcare organizations and community-based organizations in order to connect individuals that address social needs.

Integrating Clinical and Administrative Data

AHIMA supports policies that further the integration of clinical and administrative data, which can improve the patient experience, enhance efficiency, and reduce burden for providers. Processes that require the exchange of clinical data to support administrative processes generally involve a considerable amount of work, including phone calls, use of payer portals, and faxes. Prior authorizations (PA) for tests, procedures, and medications, inpatient authorizations, and medical necessity reviews, all impose significant burdens on providers and patients and raise administrative costs. In some cases, they can also delay treatment and negatively impact patient outcomes.[3] AHIMA recommends that Congress:

- Pass the Improving Seniors' Timely Access to Care Act which seeks to improve processes for patients and providers, including removing unnecessary steps and complications for patients, while decreasing administrative burdens for providers. This legislation gained overwhelming bipartisan support and passed the US House of Representatives in the 117th Congress. The bill would contribute to improving many of the burdens listed above by requiring the US Department of Health and Human Services (HHS) to establish an electronic prior authorization process for Medicare Advantage (MA) plans, establish a process for "real-time decisions" for items and services that are routinely approved, and improve transparency by requiring MA plans to report on the extent of their use of prior authorization and the rate of approvals or denials.

Health Information held by HIPAA Non-Covered Entities

The state of health data privacy in the US is rapidly evolving as the digitization of the healthcare sector accelerates. Historically, the US has followed a patchwork approach, applying sector-specific approaches to data privacy, versus a single data privacy regime. HIPAA governs health privacy in traditional healthcare settings. However, an increasing number of consumer-facing technologies, applications, products, and services that access, produce, and manage health information are not bound by or required to abide by the rules established under HIPAA, because they are not considered "covered entities" or "business associates." Rather, the privacy practices of such applications, products, and services are generally regulated by state law and/or the Federal Trade Commission (FTC) Act. This oversight does not provide the same type or level of protections for consumers as HIPAA. Therefore, in protecting health information held by HIPAA non-covered entities, AHIMA recommends that policy creates a privacy framework that does not hinder existing HIPAA framework, but includes:

- Data minimization provisions to ensure unnecessary data is not collected or used;
- Implementation of Privacy by Design policies;

---

[3] 2021 AMA Prior Authorization (PA) Physician Survey: https://www.ama-assn.org/system/files/prior-authorization-survey.pdf

- Transparency provisions that provide individuals with privacy policies detailing data collection, processing, transfer, and security activities in a readily understandable manner; and
- Data security standards relative to type of entity and data collected.

Cybersecurity and Information Security

Data breaches are an ever-growing threat in healthcare. The average total cost of a data breach in the healthcare industry was $10.1 million in 2022 — an increase of 41.6% since 2020, and making it the twelfth year in a row healthcare breach costs have been the most expensive industry for cyber breaches.[4] The healthcare sector today continues to face challenges in information sharing. While steps have been taken to increase cybersecurity, there is still a patchwork of laws and regulations and a lack of resources that must be improved and harmonized. As Congress tackles the issue of cybersecurity and information security within the health sector, AHIMA recommends that policy:

- Work to ensure health organizations are not beholden to inconsistent, duplicative or conflicting data protection standards of compliance between state and federal regulations;
- Reexamine the HHS Breach Portal, including by differentiating between health organizations that are the victim of a breach but work in good faith to protect patient data by implementing industry standard cybersecurity best practices, and those organizations who do not work in good faith to protect against a breach, as well as providing processes for health organizations to remove their name from the list demonstrating that security issues have been resolved and appropriate tools and protocols have been implemented;
- Provide federal funding or incentives for new training programs specific to training those new to healthcare cybersecurity, but also for training or certifications specific to professionals already in areas such as healthcare information security, cybersecurity, privacy, and health information management, to encourage advanced cybersecurity skills and upskill the current workforce, and;
- Prioritize engagement of all healthcare industry stakeholders and align with cross-sector cyber threat information sharing activities, ensuring information is tailored toward multiple levels of organizational size, capacity, and venue, and implemented consistently while preserving patient confidentiality and privacy.

Telehealth

With the onset of the COVID-19 pandemic, the Centers for Medicare and Medicaid Services (CMS) undertook a series of steps to expand telehealth services for Medicare beneficiaries under the Stafford Act and the National Emergencies Act. The following provisions from those waivers were extended until the end of 2024 in the omnibus passed at the end of the 117th Congress:

- Expanding originating and geographic site to include anywhere the patient is located, including the patient's home;
- Expanding eligible practitioners qualified to provide telehealth services;
- Expanding the ability for federally qualified health centers (FQHCs) and rural health clinics (RHCs) to provide telehealth services;
- Delaying the in-person requirements for mental health services provided through telehealth;
- Extending coverage and payment for audio-only telehealth services, and;
- Extending the "Hospital at Home" initiative.

---

[4]IBM Security: Cost of a Data Breach Report 2022. Available at: https://www.ibm.com/reports/data-breach.

AHIMA was pleased to see the extension of these waivers, and calls upon Congress to make these waivers permanent prior to their expiration at the end of 2024.

Public Health

Public health is a vital component of our health system, and AHIMA encourages policies around public health to ensure the soundest, most reliable, and responsible use of health information. For too long, our public health system has been underfunded and has had to contend with inaccurate and incomplete patient data in electronic health records (EHRs), inconsistent and duplicative data reporting requirements at the state and federal level, and inadequate patient privacy and security protections. AHIMA strongly recommends that policies around public health:

- Encourage standards to ensure accurate and timely data are used for public health responses and initiatives;
- Adequately fund public health infrastructure to improve interoperability and sharing of public health data;
- Adopt modern technical standards and requirements to enhance interoperability, decrease unnecessary reporting duplication, and ensures data is consistent, comparable, and meaningful across the US and internationally;
- Enhance communication and transparency with patients, and;
- Protect patient privacy and security.

Thank you for your leadership and attention to the many pressing health issues the country contends with today. We encourage Congress to ensure that health information is a central tenet while addressing these health issues. If you have any questions, please contact AHIMA Director of Government Affairs, Kate McFadyen, at kate.mcfadyen@ahima.org. We look forward to working with your offices to bolster the use of accurate, timely, trusted, and complete health information in our nation's health system.

Sincerely,

Lauren Riplinger, JD
Chief Public Policy & Impact Officer
American Health Information Management Association