Statement of the College of Healthcare Information Management Executives

House Committee on Ways and Means
Subcommittee on Social Security
House Committee on Oversight and Government Reform
Subcommittee on Information Technology

Hearing on "Protecting Americans' Identities: Examining Efforts to Limit the Use of Social Security Numbers"
1100 Longworth

May 23, 2017

The College of Healthcare Information Management Executives (CHIME) welcomes the opportunity to submit a statement for the record for the May 23, 2017, hearing entitled, "Protecting Americans' Identities: Examining Efforts to Limit the Use of Social Security Numbers." We appreciate the committees' interest in securing and protecting identities across the economy. The use of social security numbers (SSNs) in healthcare is not just common, but frequent. The use of and reliance on SSNs in the provision of care is a direct result of language that has been included in appropriations bills since 1998.

CHIME is an executive organization serving more than 2,300 chief information officers (CIOs) and other senior health information technology leaders at hospitals and clinics across the nation. CHIME members are responsible for the selection and implementation of clinical and business technology systems facilitating healthcare transformation. Our organization is a strong proponent of health IT and its ability to enable improvements in health care quality, increase affordability and improve healthcare outcomes.

Why are SSNs used in Healthcare?
There is no standard for patient identification in the United States. Common practice today is to identify patients based on name and one or more personal identifiers, such as date of birth or street address and often social security number. Unfortunately, name and date of birth offer no guarantee of accurate identification and often providers differ in how they record and store identifying information so other data elements, including SSN are leveraged. As patients visit multiple providers and records are exchanged, ensuring accurate identification is essential. With the growth of electronic health records, however, there is a greater risk of error if the bits and bytes do not match up.

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 said, "The Secretary [of Health and Human Services] shall adopt standards providing for a standard unique health identifier for each individual, employer, health plan and health care provider for use in the health care system.[1]"

[1] Section 262 (Sec 1173), Title II, Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191), August 21, 1996.

The Congressional mandate for a unique health identifier was halted in 1998 by then-Representative Ron Paul (R-TX) with the insertion of a funding prohibition into the Department of Labor and Health and Human Services (Labor-HHS) appropriations bill, "None of the funds made available in this Act may be used to promulgate or adopt any final standard under section 1173(b) of the Social Security Act (42 U.S.C. 1320d–2(b)) providing for, or providing for the assignment of, a unique health identifier for an individual (except in an individual's capacity as an employer or a health care provider), until legislation is enacted specifically approving the standard.[2]"

The language supported by Representative Paul has remained in every funding bill since fiscal year 1999, with clarification on Congress' intent just offered in the committee report accompanying the FY2017 Omnibus Appropriations Act passed earlier this month. The committee report offered two instances of clarification and direction to the federal government concerning the issue of patient identification:

> "Unique Patient Health Identifier. —The Committee is aware that one of the most significant challenges inhibiting the safe and secure electronic exchange of health information is the lack of a consistent patient data matching strategy. With the passage of the HITECH Act, a clear mandate was placed on the Nation's healthcare community to adopt electronic health records and health exchange capability. Although the Committee continues to carry a prohibition against HHS using funds to promulgate or adopt any final standard providing for the assignment of a unique health identifier for an individual until such activity is authorized, the Committee notes that this limitation does not prohibit HHS from examining the issues around patient matching. Accordingly, the Committee encourages the Secretary, acting through the Office of the National Coordinator for Health Information Technology and CMS, to provide technical assistance to private-sector led initiatives to develop a coordinated national strategy that will promote patient safety by accurately identifying patients to their health information.[3]"
>
> "Electronic Health Records. —The Committee believes HHS' work to encourage the adoption of electronic health records has provided important new opportunities to improve the quality, safety, and cost-effectiveness of health care. The Secretary is directed to further this work by studying approaches to improve person-centered healthcare through patient access to health information. That work should examine accurate and timely record matching so that all EHR systems are collecting the information necessary for a fully interoperable system that protects patients from identity mismatch errors, but also considers patient privacy and security. [4]"

The Current Use of SSNs in Healthcare

SSNs were first issued in the 1930s as a means to track and calculate retirement benefits. Today, however, the SSN has become a de facto national identifier. The lack of a universally-adopted healthcare identification solution has resulted in healthcare providers requesting SSNs as a factor in identifying the patient presenting for care. However, healthcare providers are unable to employ SSNs in a healthcare setting as the sole identifier given that individual states have enacted laws restricting their use in certain circumstances, healthcare provision being one of them. Medicare and Medicaid programs, being government programs, however, are able to use SSN for identification, but private sector entities in most circumstances may not mandate the collection of SSNs.

The existing identity theft threats have only contributed to the concerns about use of SSNs in healthcare, especially given the personal nature of health information. Under current rules, patients

[2] Original Language - Section 516, Title V, Omnibus Consolidated and Emergency Supplemental Appropriations for FY 1999, H.R. 4328 (P.L. 105-277), October 21, 1998

[3] https://www.congress.gov/114/crpt/hrpt699/CRPT-114hrpt699.pdf

[4] https://www.congress.gov/114/crpt/srpt274/CRPT-114srpt274.pdf

are not required to submit their SSN for treatment, and may only submit the last four numbers or in some cases they are permitted to submit incorrect digits just to satisfy a field. Thus when SSNs are included among the data points a healthcare provider is using to identify a patient, only having the last four digits or false digits only contributes to the difficulty in identifying the patient seeking care.

Decreasing the Use of SSNs for Healthcare
While healthcare providers will continue capturing SSNs to facilitate patient identification using algorithms, there are efforts to reduce its overall use.

In the Medicare Access and CHIP Reauthorization Act (MACRA) of 2015, Congress directed Congress to remove SSNs from Medicare beneficiary cards by April 2019[5]. This resulted in the Social Security Number Replacement Initiative (SSNRI) underway at the Center for Medicare and Medicaid Services (CMS). CMS has opted to issue an alphanumeric identifier to each beneficiary, called a Medicare Beneficiary Identifier (MBI.)

While the SSNRI is intended to reduce the use of SSNs in healthcare, it is only applicable to Medicare beneficiaries. Further, SSNs are still likely to be used by provider organizations in an effort to identify the patient as a legacy data point in matching algorithms. Recalculating or upgrading identification algorithms would be extremely costly for healthcare organizations.

The Costs of Maintaining the Status Quo in Patient Identification
Beyond identify theft and privacy challenges associated with the continued use of SSNs and other factors to identify patients, additional concerns should be considered by the committees. Despite using SSNs and other personal demographics to identify patients, there remains significant rates of mismatches or unmatched patient records which impact patient safety and increase healthcare costs. Examples of patient safety and financial implications for not having a healthcare specific identifier include:

- In a 2012 study, nearly 20 percent of CHIME members reported that they could trace an adverse medical event to inaccurate patient identification and matching.
- Intermountain Healthcare officials report spending between $4 million and $5 million annually to improve patient identification accuracy rates.
- In a 2014 report, the Office of the National Coordinator for Health Information Technology noted that every case of misidentification costs the Mayo Clinic at least $1,200.
- According to a study conducted at the Children's Medical Center in Dallas,[6] a database with approximately 1 million records, or unique patients, may include up to 120,000 duplicate records. The study found that these duplicate records cost healthcare organizations about $96 per duplicate record. In 4 percent of cases involving confirmed duplicate records, clinical care was negatively affected. Care quality issues included duplicated tests due to lack of access to previous test results, and delays in surgery due to lack of patient history and physical reports. On average, repeated tests or treatment delays added $1,100 to the cost of the patient's care.

Enabling a Healthcare-specific Identifier
Reducing the reliance on SSNs and other identifiable information that help bad actors execute fraud will immediately devalue health records on the black market. We need a healthcare identification solution that, if stolen, does not have the same potential for fraud and abuse. It is essential that Congress remove the language in the Labor-HHS Appropriations bill prohibiting HHS (in Sec. 510) from using any federal funds to "promulgate or adopt any final standard …. providing for the assignment of a unique health identifier for an individual."

[5] Sec 510. Medicare Access and CHIP Reauthorization Act of 2015. H.R. 2 https://www.congress.gov/114/plaws/publ10/PLAW-114publ10.pdf
[6] Beth Haenke Just et. al., Why Patient Matching Is a Challenge: Research on Master Patient Index (MPI) Data Discrepancies in Key Identifying Fields (2016).

Technology has provided for alternatives to a numeric or alphanumeric identifier as a solution, and the government does not need to be the arbiter of the identification solution, but HHS must be able to provide technical assistance to private sector initiatives. Unfortunately, HHS has interpreted the annual funding ban to prohibit them from collaborating or assisting with private sector efforts to improve patient identification on a national level.

As health information increasingly flows across unaffiliated providers in order to coordinate care and as patients increasingly access and share their own data, it becomes even more important to ensure that patients are accurately identified and matched to their data. Ensuring patients are correctly matched to their records is the first step toward effectively protecting and securing identities and mitigating fraud. CHIME encourages committee members to work with the relevant appropriations committees to remove or amend the federal funding prohibition that has contributed to the frequent use of SSNs to identify a patient.

Recognizing that the industry can no longer wait, CHIME, through its Healthcare Innovation Trust, has launched a $1 million crowd-sourcing challenge to find a safe, private and secure approach to ensure accurate patient identification. The first phase of the competition saw 113 innovators from around the world submit ideas; more than 340 individuals and teams from 39 countries have registered for the National Patient ID Challenge. Four finalists were announced on May 15, 2017 to proceed to prototype testing. The solutions range from block chain to various biometric technologies as a means to satisfy the 100 percent identification mandate. The CHIME Healthcare Innovation Trust will announce a final solution in November 2017.

It's clear that private sector solutions exist and we encourage HHS to work with the private sector to develop or disseminate a unique health identification solution. As evidenced by the CHIME Healthcare Innovation Trust National Patient Identification Challenge, the private sector can and should take a leadership role in addressing this issue, but it will be imperative that HHS be engaged in the conversation and be allowed to provide technical assistance to ensure an industry-adopted solution also meets the needs of the federal government for care delivery and reimbursement purposes.

As the committees evaluate how to better leverage technology as a means to reduce the reliance on SSNs across the federal government and in the provision of healthcare, members should evaluate the role of the HHS funding prohibition has played to halt progress across the industry and the impacts on patient care. Members can also consider what technological alternatives exist beyond the assignment of a numeric, or alphanumeric identifier, for use in healthcare. Issues of fraud, identity theft and unlawful access to care are exacerbated by the lack of a coordinated national strategy for patient identification.