Removing the Appropriations Ban on a Unique Patient Identifier: Responding to Concerns Expressed by Supporters of Maintaining the Ban
April 2020

Introduction: Today, there is no consistent and accurate way of linking a patient to their health information as they seek care across the health care continuum. Countless times every day a patient record is mismatched or goes unmatched. Serious patient safety concerns arise when data is mismatched or important data is missing.

Common to every health system across the country are terrible stories: mammogram results filed into the wrong patient's record, only to be discovered when the patient was terminal; babies receiving incorrect milk; inappropriate medications being delivered; and opiates being prescribed to patients with a history of addiction. All of these episodes occur simply because – at present – we cannot fully identify the right patient at the point of care and link their prior care records. According to a *2016 National Patient Misidentification Report,* 86 percent of respondents said they have witnessed or know of a medical error that was the result of patient misidentification.[1]

Currently, there is no standard for patient identification in the United States. Indeed, the United States is the last industrialized nation without a national unique identification system.[2] As a result, health care organizations must rely on a variety of processes and technologies including patient matching algorithms driven by varying combinations of patient demographic data elements and other identifiers.[3] Because the U.S. lacks a standard, we must rely on slippery identifiers such as date of birth or names. Unfortunately, name and date of birth offer no guarantee of accurate identification, and providers compound the identification dilemma because they differ in how they record and store identifying information.

Efforts to address the ongoing coronavirus pandemic underscore the importance of a national solution that enables patient health data to be accurately identified to the correct patient. Makeshift hospitals and hastily established testing sites in parks, convention centers and parking lots challenge the ability of health care providers to ensure that patient data is linked to the correct patient. Indeed, simply enabling access to electronic health records in these non-traditional settings is a major undertaking. For example, we have heard reports of instances where patient specimens are collected for COVID-19 testing in temporary sites and then sent off-site to a public health agency for testing and the results returned have been difficult to match to the correct patient given the scant amount of identifying information included with the sample.

Now more than ever, accurate identification is essential. With greater mobility, the movement to value-based payment, and advances in health data exchange, more patient health records are being exchanged, accessed, and used. This is why it is increasingly important that bits and bytes match up. Take for example, Harris County Hospital District. In 2011, hospital district officials found 3.4 million patients in the database. Of that number, there were 249,213 instances where patients shared the same first and last name. There were nearly 70,000 instances where two or more patients shared the same name and date of birth. In fact, according to Harris' CIO, 2,488 people were found named Maria Garcia, 231 of whom had the same birthday.[4] This example highlights the need to take steps to ensure that we are treating the right patient at the point of care.

---

[1] 2016 National Patient Misidentification Report, Available at: https://pages.imprivata.com/rs/imprivata/images/Ponemon-Report_121416.pdf.
[2] Grannis, S.J. et al, 2019, 'Evaluating the effect of data standardization and validation on patient matching accuracy', *Journal of the American Medical Informatics Association*, vol. 26, no. 5, pp. 447-456.
[3] Ibid, 448.
[4] Available at: https://healthsystemcio.com/whitepapers/PatientSecure-WhitePaper-Imprivata.pdf.

Congressional Activity: Congress has significantly invested in national health information exchange. With the passage of the Health Information Technology for Clinical and Economic Health (HITECH) Act in 2009, Congress placed a clear mandate on the Nation's health care community to adopt electronic health records (EHRs). The 2016 21st Century Cures Act further advanced interoperability of health data and took steps to prevent health care providers and EHR vendors from inappropriately blocking information flows.

Without a national strategy for patient identification, however, we will not be able to realize the congressional intent of HITECH and 21st Century Cures—true nationwide data interoperability and transformation of the Nation's health care delivery system.

On June 12, 2019, the U.S. House of Representatives acted in bipartisan fashion to remove the longstanding appropriations ban on funding for a unique patient health identifier when an amendment to strike the ban offered by Representatives Bill Foster (D-IL) and Mike Kelly (R-PA) passed in a 246-178 vote. While the ban was not removed in the final HHS funding bill, the Further Consolidated Appropriations Act, enacted into law on December 20, 2019 (P.L. 116-94), included important report language, set forth below:

Office of the National Coordinator for Health Information Technology (ONC)

Patient Matching. – The general provision limiting funds for actions related to promulgation or adoption of a standard providing for the assignment of a unique health identifier does not prohibit efforts to address the growing problems faced by health systems with patient matching. The agreement encourages HHS to continue to provide technical assistance to private-sector-led initiatives to develop a coordinating national strategy that will promote patient safety by accurately identifying patients to their health information. Additionally, the agreement directs ONC, in coordination with other appropriate Federal agencies, to provide a report to the Committees one year after enactment of this Act studying the current technological and operational methods that improve identification of patients. The report shall evaluate the effectiveness of current methods and recommend actions that increase the likelihood of an accurate match of patients to their health care data. Such recommendations may or may not include a standard for a unique patient health identifier. The report shall include the risks and benefits to privacy and security of patient information.

The following section seeks to address specific concerns of the ACLU and FreedomWorks about a unique patient identifier as enumerated in an October 19, 2019 letter to Congress.

Concern: *Removing Sec. 510 would eliminate Congress' role in approving unique health identifier standards, potentially paving the way for a de facto national medical ID system, absent Congressional approval. The dangers of having a system like this compromised, inappropriately used, or accessed to track individuals are profound.*

Response: Removal of the ban would reinstate the status quo set forth in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which includes clear instructions to the Secretary of HHS to adopt standards for health data while protecting its privacy and security with appropriate safeguards against misuse or threats to data integrity. As HIPAA states:

> *"The Secretary 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."*

Removal of Section 510 would in no way limit Congress' ability to enumerate the powers, duties and functions exercised by Federal agencies, as well as Congress' ability to counteract through subsequent legislation agency actions implementing its delegated authority.

The ban has arguably led to an "inverse" privacy problem – whereby individuals must repetitively disclose individually identifiable information to each health care provider they see. A national patient identification strategy is needed to keep each individual's data private and separate from other individuals' data. This would enable avoidance of avoid "false positives" (i.e., where a health care provider improperly discloses a patient's health information to another patient with the same name) and "false negatives" (i.e., where a health care provider maintains multiple medical records for the same individual because the system is unable to correctly match the individual to his or her existing record).

Concern: *Absent strong privacy protections, use of unique health identifiers could empower HHS and potentially other federal agencies (including law enforcement) to gain unprecedented access to sensitive medical information.*

Response:
When inclusion of the ban was first suggested more than two decades ago, the stringent privacy and security protections in the Health Insurance Portability and Accountability Act (HIPAA) were not yet effective. Today, the HIPAA Privacy and Security Rules establish a national standard to limit the use and disclosure of individuals' electronic medical records and other protected health information by health plans, health care clearinghouses, health care providers that conduct standardized electronic health care transactions (e.g., claims and eligibility transactions) and their business associates.

The creation of a UPI standard will not give any Federal agency, including Federal law enforcement agencies, additional access to individually identifiable health information. The Privacy Act of 1974 protects government-maintained records about individuals retrievable by personal identifiers such as name, social security number or other "identifying particular assigned to the individual."[5] Prior to using an individual's UPI or other individually identifiable health information to create a new "system of records", the requesting Federal agency would be required to publish a "System of Records Notice" in the Federal Register that would explain the purpose for creating the system of records and the specific steps taken by the Federal agency to protect the privacy and security of such records.

Any such System of Records Notice would be subject to notice and comment. If a Federal agency were to create a System of Records containing the UPI for a purpose permitted under its congressional mandate, not only does an individual have the right to an account for disclosures of any records maintained about him or her but the Act prohibits the disclosure of such records without the prior written consent of the individual to whom the record pertains unless certain exceptions delineated in the Privacy Act apply.[6] These protections would prevent agencies from using their mere access to the UPI assigned to individuals to indiscriminately request and receive other individually identifiable health information about individuals.

Recall that the bipartisan Medicare Access and CHIP Reauthorization Act of 2015 established a Medicare Beneficiary Identifier (MBI) for all current and past Medicare beneficiaries. Congress did not identify what privacy and security protections should be implemented for the MBI, nor did they dictate what should ultimately replace the Social Security number on Medicare cards; rather, Congress entrusted the US Department of Health and Human Services (HHS) to do so. Further, servicemen and women, as well as veterans, have a unique health identifier that was not informed by Congress.

---

[5] 5 USC § 552a(a)(4).
[6] Available at: https://www.hhs.gov/foia/privacy/index.html.

Concern: *Historically, we have seen examples of inadequate health privacy regulations, underscoring the importance of requiring Congressional approval of health privacy standards in this arena. For example, in 1999 the Center for Disease Control and Prevention (CDC) issued draft guidance recommending states institute case reporting of individuals who tested positive for HIV, supporting a name-based identification system. Previously, HHS has issued proposed regulations that would give law enforcement officials unfettered access to patient medical records, without requiring patient consent. Given this history, it is critical that any regulations permitting a unique health identifier be approved by Congress.*

Response: Removal of Section 510 from the bill in no way limits congressional authority in legislating the adoption of health privacy standards. Furthermore, the examples provided here both occurred prior to the enactment and implementation of the Health Insurance Portability and Accountability Act (HIPAA). HHS has explicitly stated that the HIPAA Privacy Rule does not require a physician or any other covered entity to send medical information to the government for a government database or similar operation. The Privacy Rule does not require or allow any new government access to medical information UNLESS the Office for Civil Rights (OCR) is investigating complaints that the Privacy Rule protection or rights have been violated to ensure that covered entities comply with HIPAA. Even so, the HIPAA Privacy Rule limits disclosures to OCR to information that is "pertinent to ascertaining compliance."[7]

The HHS Office for Civil Rights also notes, "the [HIPAA Privacy] Rule does not expand current law enforcement access to individually identifiable health information. In fact, it limits access to a greater degree than currently exists, since the Rule establishes new procedures and safeguards that restrict the circumstances under which a covered entity may give such information to law enforcement officers."[8]

Furthermore, identifiers are currently in use in the Medicare population as directed by Congress in 2015 and in use by the Department of Veterans Affairs (VA) and the Department of Defense. Indeed, by all accounts, the rollout of the UPI for Medicare beneficiaries has been highly successful. While inclusion of the MBI on Medicare FFS claims was not required until January 1, 2020, 86% of FFS claims submitted in December 2019 included the MBI. Again, no evidence to date suggests these existing programs have encouraged unfettered access to an individual's health information.

Concern: *Existing law does not prohibit HHS from studying or examining the uses of unique health identifiers to inform future legislation. The House Appropriations Committee made this clear in the FY 2019 Labor-HHS Appropriations bill, stating "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." The Committee encouraged HHS to "provide technical assistance to private-sector-led initiatives to develop a coordinated national strategy" for the purpose of promoting patient safety.*

Response:
Unfortunately, HHS's interpretation of the prohibition over the past two decades has effectively curtailed, if not shut down, the study, discussion, and examination of the use of unique health identifiers. The limited study and examination that has taken place has not translated into the advancement or adoption of a nationwide patient identification strategy that enhances patient safety. In the meantime, without the ability for clinicians to correctly connect a patient with their medical record, lives have been lost and

[7] Available at: https://www.hhs.gov/hipaa/for-individuals/faq/347/does-hipaa-require-my-doctor-to-send-my-medical-records-to-the-government/index.html.

[8] Available at: https://www.hhs.gov/hipaa/for-individuals/faq/349/will-hipaa-make-it-easier-for-law-enforcement-to-get-my-medical-information/index.html.

medical errors have needlessly occurred. These are situations that could have been entirely avoidable had patients been able to have been accurately identified and matched with their records.

The aforementioned FY 2020 report language does enable a thorough examination of the UPI. Congress specifically directs ONC to study current technological and operational methods that improve identification of patients and to evaluate the effectiveness of these methods and the risks and benefits to privacy and security of patient information. The report shall also make specific recommendations to Congress that increase the likelihood of an accurate match of patients to their health care data.