Myth vs. Fact: Removing the Appropriations Ban on a Unique Patient Identifier

The inability to engage in a nationwide dialogue on patient identification has resulted in the loss of American lives. Common to every health system across this country are terrible stories: mammogram results being 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. In the absence of a standard, the common practice is to rely on slippery identifiers such as date of birth or street address. 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.

Now more than ever, accurate identification is essential. With greater mobility, Americans are visiting multiple providers, and more records are being exchanged, accessed, and used. In addition, the growth of electronic health records over the last decade makes it essential 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.[2]

Congress has moved in the right direction on national health information exchange over the last five years, especially with a 21st Century Cures Act that paved the way for interoperability. But without a national strategy for patient identification—which is what the Foster-Kelly Amendment allowed for--we will not be able to realize the congressional intent of the Cures Act—true nationwide data interoperability.

Simply put, we must ensure that we are treating the right patient at the point of care.

The following myths and facts aim to address common misconceptions about a unique patient identifier.

Myth: *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.*

Fact: 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 that would protect the privacy and security of the data 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."*

---

[1] 2016 National Patient Misidentification Report, Available at: https://pages.imprivata.com/rs/imprivata/images/Ponemon-Report_121416.pdf.

[2] Available at: https://healthsystemcio.com/whitepapers/PatientSecure-WhitePaper-Imprivata.pdf.

Prior to the congressional ban, a comprehensive analysis of unique patient identifier (UPI) options, commissioned by HHS, supported the use of a UPI. That study concluded that – among its strengths – the UPI would provide accurate identification without the "repetitive use and disclosure of an individual's personal identification information," thereby preserving anonymity, protecting privacy, and preventing unauthorized access to health information.

As a result, the ban has led to an "inverse" privacy problem – and a national patient identification strategy is needed to keep each individual's data private and separate from other individuals' data. Furthermore, while individuals have a protected privacy right with respect to their own data, they do not have a right to be ambiguous with respect to their data, because ambiguity can threaten the integrity of other individuals' data.

Myth: *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.*

Fact: The 2015 Medicare Access and CHIP Reauthorization Act (MACRA) 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.

Myth: *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.*

Fact: 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 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."[3]

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."[4]

---

[3] 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.

[4] 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.

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.

Ultimately, patient matching is, fundamentally, a safety issue. Patient information needs to be identified to the correct patient and/or identified to the correct patient but not in a duplicate/incomplete record. The ability to use a health identifier will also be critical for social determinants of health and other population-based health care delivery.

Myth: *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.*

Fact: While the appropriations report language, not bill text, has allowed the Office of the National Coordinator for Health IT (ONC) and the Centers for Medicare and Medicaid Services (CMS) to work on patient matching, HHS remains prohibited from exploring any unique identifier.

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 solution 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 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 terms "patient matching" and "patient identification" are often used interchangeably, but that is incorrect. Matching is leveraging data elements, often within one single health system, to be able to link a single patient to records from a prior encounter. Patient identification denotes the ability to have a single solution that points back to one individual that transcends care locale.

The absence of a national strategy for uniquely identifying patients has resulted in significant costs to hospitals, health systems, and their efforts to facilitate health information exchange. With the proliferation of electronic health records and the national drive toward interoperability, accurately matching patients to their data is more important now than ever before.

With respect to the privacy and security of implementing a unique identifier, a study reviewed the European experience with UPIs to date and found no significant breaches of the security of individual health information and only limited concerns about a UPI among patients. The same study also found that it is possible through the implementation of a UPI to enhance the protection of personal health information by encrypting other personal attributes.