Finding John Doe: Patient Matching and the Need for a National Health Safety Identifier

By Mary Butler

Over the past several years it's been hard to avoid public conversations about the "childhood obesity epidemic." One of the biggest targets for regulators like the USDA and for politicians such as former New York City Mayor Michael Bloomberg has been Americans' addiction to sugary beverages.

Bloomberg famously tried—and failed—to ban the sale of soft drinks sized over 16 ounces in New York three years ago based on a vast body of evidence and research linking soft drinks, fruit juices, and energy drinks to high rates of obesity in the United States. Bloomberg's reasoning made sense on paper. According to research published in 2012, with each additional 12-ounce soda children consume each day the odds of becoming obese increased by 60 percent during 1.5 years of follow-up.[1] First Lady Michelle Obama has also taken up the fight against sugar-laden beverages in her "Let's Move" anti-obesity campaign.

Bloomberg and Obama, so far, are seeing mixed results with their efforts, but one thing is for sure: Americans are hearing the debates and paying attention, regardless of how inclined they are to listen to the advice of politicians—not to mention their doctors.

Imagine, though, what the world would be like if the powerful beverage industry lobby groups were able to convince lawmakers to outlaw the expending of federal resources to further research the link between obesity and sugary drinks. This could hinder research into the development of treatments for diabetes and heart disease, as well as lead to higher healthcare costs in the future.

Thankfully, there is no federal ban like the hypothetical one discussed above. But there is a very real prohibition on federal dollars being spent on a topic near and dear to the hearts of health information management (HIM) professionals: the use of a unique patient identifier (UPI) to confirm an individual's identity in a healthcare setting. And while sugary drinks can harm your health, so too can misdirected and misidentified health information. In fact, putting the wrong information in the wrong medical record can kill.

When HIPAA was drafted in 1996, it included a provision that required the US Department of Health and Human Services (HHS) to "adopt national standards for electronic healthcare transactions" and "a standard unique health identifier for each individual, employer, health plan, and health care provider for use in the health care system." But in 1998, amidst warnings from privacy activists and lawmakers concerned about the encroachment of "Big Brother," and fears that a national UPI would be misused, Congress passed Public Law 105-277, which prohibits HHS from dedicating resources to "promulgate or adopt any final standard… providing for, or providing for the assignment of, a unique health identifier for an individual… until legislation is enacted specifically approving the standard." This law has been carried forward as part of a federal appropriations bill ever since.

Twenty years later the healthcare industry is still struggling with how to properly identify patients. However, officials at AHIMA are optimistic that consumer perspectives have changed and that it's time to revisit the national conversation about patient identity.

This spring, AHIMA plans to petition the White House and ask President Obama to help lift the federal ban through a grassroots advocacy campaign called MyHealthID. Meanwhile, in absence of a UPI, some providers, health information exchanges (HIEs), health IT trade organizations, and health IT vendors aren't waiting for Congress or the president to act and instead are collaborating on their own patient identity solutions.

AHIMA Takes the Lead

HIM professionals are the experts when it comes to making sure patients are properly identified at registration and, most importantly, at the point of care, says Pamela L. Lane, MS, RHIA, CPHIMS, vice president of policy and government relations at AHIMA, who is spearheading the MyHealthID campaign.

Results of a new survey conducted by AHIMA demonstrate the extent to which HIM is involved in reconciling duplicate records.[2] The survey polled 815 AHIMA members who used 12 different electronic health records systems (EHRs) between them. The survey found that 57 percent of respondents reported working on possible duplicates regularly, with 73 percent saying they work on possible duplicate records at least once a week. This duplication management process is labor intensive and time consuming. It is also greatly hindered by staff turnover, lack of executive support, and the absence of good information governance policies, according to respondents.

A voluntary patient safety identifier would go a long way towards easing the administrative burden of duplicate records, according to Lane and the authors of AHIMA's survey. If every consumer had their own number, that would help ensure that nurses and physicians have access to a patient's medical history and test results at crucial times. The patient safety implications of misidentifying patients—of confusing one John Doe with another John Doe—are huge, and that's the point AHIMA plans to make in its campaign.

Many kinds of mistakes can be made when multiple records are created for the same person, Lane says. "Because let's say you have two health records. The older record had your medication allergies recorded in it, but the new one doesn't. Until that info gets merged into the new record, if you have an allergy and forget to tell a provider they don't have those pieces tied together. That's a huge patient safety issue," Lane says.

Another example—John Doe is taking a medication that is contraindicated with certain pain medications or anesthetics and is admitted to the hospital through the emergency department. Doe lacks a driver's license or other forms of ID with key identifiers. Even if Doe's been a patient at this hospital before, there could be hundreds of other John Does with his birthday in the system. If he's given one of the contraindicated medications prior to emergency surgery, he could die. However, if Doe had another existing number that could be used as a UPI instead of just his name and date of birth, treating physicians would know for certain that they're treating the right John Doe and would be able to spot the complication at the point of care.

With the advent of electronic records, it's easier for consumers to see how easily they could be confused for someone else. Nearly everyone has received an errant e-mail intended for someone with a similar name or e-mail address. And plenty of consumers know two different people with the same name. It is a low-stake mistake when an e-mail is misdirected, but when dealing with misdirected health information, the mistake can have serious consequences.

"I think everybody gets it now. If we had tried to explain this [using a voluntary patient safety identifier] years ago, they would not have gotten it. But in today's electronic world if they don't identify you correctly, information is just flying around everywhere," Lane says.

Giving individuals unique identifiers would also help health information exchange and improve interoperability, which is a priority for the Office of the National Coordinator for Health IT (ONC). But again, Public Law 105-277 makes such discussions off limits to those who are best positioned to tackle the matter. Lane says she has heard of instances in which work groups comprised of government employees and private stakeholders have come to a screeching halt and disbanded the minute someone mentions a national UPI—all due to Public Law 105-277.

"How silly is that?" Lane says. "The federal government needs to be at the table, they need to be participating… We're going to ask consumers to acknowledge this is important, they get this, they get how confusing it is. What they don't know is that the federal government is prohibited from finding a solution."

AHIMA's view is that an online petition on the White House's website, and the advocacy work it will take to get people to sign it, will build consumer awareness of the patient identity matching problem. According to the guidelines of the White House's petition website, located at petitions.whitehouse.gov, Obama Administration officials guarantee a formal response to parties who are able to get 100,000 signatures in 30 days.

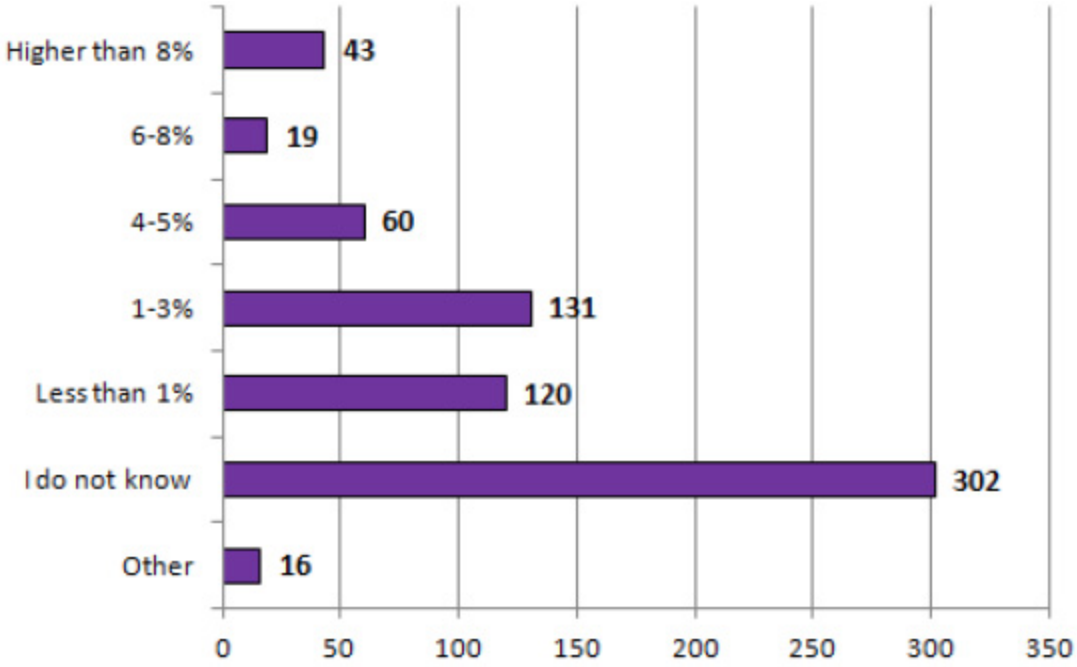
AHIMA's petition won't propose a solution to patient identity matching, but merely propose that the ban against discussing a national UPI be lifted and suggests that a patient safety identifier, if adopted, should be voluntary for consumers. Lane hopes that by making the use of a patient safety identifier voluntary, consumers will be less worried that the government is creating another way to track them. If a person opts to create a voluntary patient safety identifier, it's up to them with whom to share it under AHIMA's proposal.

The petition will be posted online on March 20 with a window for signatures ending on April 19. With the petition, AHIMA is looking to jump start a wider collaboration toward a solution. After all, it's hard to have a conversation about an issue with national implications without having the federal government involved, Lane says.

While Lane is confident that AHIMA will be able to meet the 100,000 signatures requirement, the question becomes: what comes next? Lane says there is an understanding that AHIMA has no control over how the White House responds to the petition. President Obama may or may not be moved to urge Congress to consider legislation to lift the ban.

"Even if we didn't get 100,000 signatures, even if we get 90,000, it has brought attention. We've educated the public and called attention to the issue. And we have said 'AHIMA is standing by and will take the lead in working with whomever to fix this problem and find the solution,'" Lane says.

Survey: What is your duplicate medical record rate in your EHR?



Source: AHIMA. "Patient Matching Survey Results." Unpublished. August 19, 2015.

Private Sector May Hold Patient Matching 'Key'

The healthcare industry is far from unique in needing a method by which it can confirm the identities of consumers. Organizations in sectors such as banking and telecommunications have developed their own means of solving this puzzle.

Michael Nelson, DPM, vice president of healthcare strategy and business development, identity, and fraud solutions at Equifax, a consumer credit reporting bureau and Big Data solutions company, says identity matching is a challenge for any organization that has vast consumer databases. As a credit bureau, Equifax maintains a national database of millions of unique consumers that includes current and historic demographic information with factors such as address changes, name changes due to marriage or divorce, and new aliases, Nelson says.

"Essentially, this can serve as a referential database on a national scale. We have assigned a unique key, which serves as a data match key, to every unique consumer in our database. Hundreds of millions of them," Nelson says. "It just seems logical that if we match a healthcare organization's patient file to our referential database, and append the unique key to it, this key could be consumed by its IT system through the enterprise master patient index (EMPI); it could create a couple value propositions."

The first of those value propositions is that the data match key can be a more heavily weighted attribute in the matching algorithms of the EMPI, which would create more accurate matches and reduce the number of duplicate records created. The second value proposition, according to Nelson, is that the data match key can be used to match patient records across one or more unaffiliated organizations.

"What we often say is 'What good is interoperability if you can get two disparate systems to talk to one another but they cannot agree upon whom they're talking about?' This data match key could help facilitate health information exchange, and as it propagates out to the payers can help facilitate the matching of claims data to clinical data," Nelson explains.

Nelson notes that he does not advocate for ripping and replacing MPIs. Rather, he would like to see MPIs augmented by the data match keys, which would work behind the scenes within the organization's IT infrastructure and never be exposed to the patient. He says that even if the industry is successful in adopting a national patient identifier, there is still more work to be done because the patient's existing records must first be linked to one another and then linked to a national identifier.

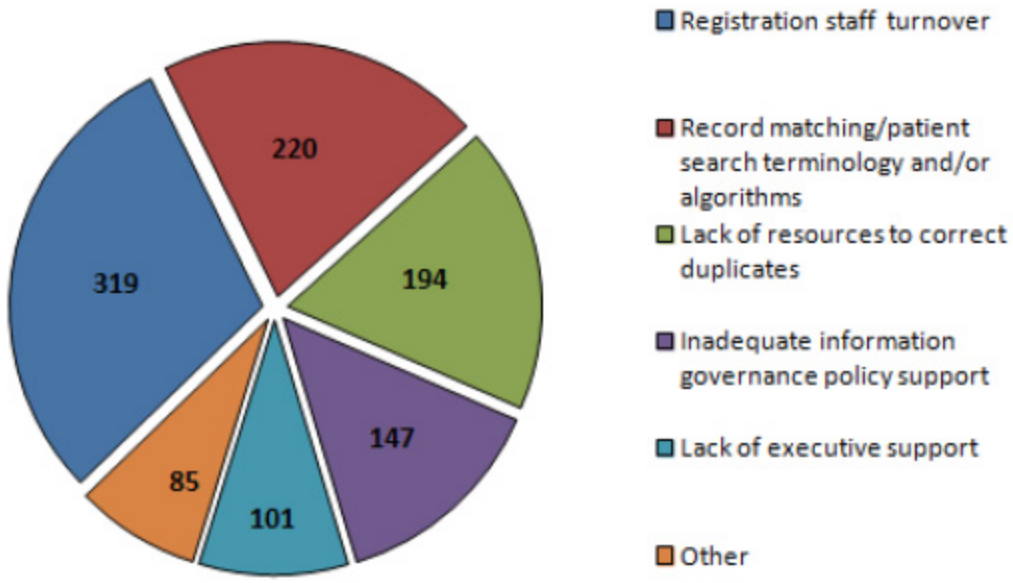
Other private organizations, such as the CommonWell Health Alliance and The Sequoia Project, are also working on their own solutions to interoperability and patient matching.

CommonWell, a nonprofit trade association with members including EHR vendors and state HIEs, for example, has launched interoperability pilot tests in cities across the country. Its services include patient identification and linking, record location and retrieval, and privacy and consent management, among others.

The Sequoia Project is another nonprofit dedicated to advancing the implementation of secure and interoperable nationwide health information exchange. At the end of 2015, the Sequoia Project and the Care Connectivity Consortium released a white paper that included a patient matching maturity model designed to help organizations assess their current state and provide a roadmap towards methodically improving patient matching. It also included a list of patient matching best practices for healthcare CIOs and CTOs.

Additionally, ONC has teamed up with the Healthcare Information and Management Systems Society (HIMSS) to develop better strategies to improve consistent patient data matching in healthcare. One of their combined projects is the creation of an Innovator-in-Residence program, which is dedicated to finding patient matching solutions. Additionally, ONC, the HHS Office of the Chief Technology Officer, and HIMSS co-sponsored a HIMSS Patient Matching Testing event in 2015 where programmers and developers experimented with patient matching algorithms in a laboratory setting.

Survey: What kind of challenges do you face on a daily basis with managing your MPI?



Source: AHIMA. "Patient Matching Survey Results." Unpublished. August 19, 2015.

Biometric Identification Shows Promise

Until there's a national consensus on the deployment of a patient safety identifier, or greatly improved health IT interoperability between providers and states, hospitals and other providers will be left trying to tackle the issue on their own. For some, that means bringing in consultants who specialize in MPI cleanups. But for others, such as Harris County Hospital District in Houston, TX, one strategy has been to deploy a biometric identification program to ensure patients are accurately identified.

In 2011 Harris County launched a palm scanner that uses infrared technology to map a patient's network of veins. The hand vein-pattern is used for identification since it is unique to each individual and does not change over one's lifetime. This technique is said to be 100 times more accurate than thumbprints, according to a Harris County press release.

The following statistics for Harris County demonstrate why a high-tech approach was warranted. In the hospital's patient database of 3,428,925 patients, there were 249,213 times when two or more patients shared the same first and last name. What's more, there were 69,807 instances in which two or more patients share the same first and last names and date of birth. For example, there were 2,488 patients named "Maria Garcia" in Harris County's system, with 231 of those Maria Garcias also sharing the same date of birth. This illustrates just how easy it can be to misdirect patient information during an episode of care.

Hoping to help, Michael Talley, director at University Bancorp of Ann Arbor, and a director of the Southeast Michigan Health Information Exchange (SEMHIE), is bringing his banking expertise and experience with two-factor authentication and biometrics to the healthcare world.

Talley says that since personal health data, like an individual's bank account information, is such a high-value target for would be hackers, it requires the highest level of protection. Experts like Talley think two-factor authentication is the best way to do this.

Two-factor authentication usually requires a user name and password, and then an additional layer of protection like a biometric, which can be a thumbprint, a palm print, or voice identification.

The use case Talley is aiming to develop and achieve at SEMHIE is to prove that a doctor, a patient, and a patient's insurance company can retrieve the right patient's lab results through an HIE with a two factor authentication process, including a biometric.

"We're not reinventing the wheel. What we're trying to do is make it as ubiquitous or as easy for people to authenticate themselves as possible, to have access to the data that they're authorized to see, [and] run the applications," Talley says.

A patient's biometric information can be obtained easily during the registration process at a hospital or doctor's office. Registration staff would have palm or thumbprint readers at their work stations with which to gather the patient's print while registering. That print is then converted to a digital signature that generates a file that can be transferred to the patient's mobile device, including their tablet, laptop, or smartphone, or a basic cell phone. That biometric identifier, when used with another two-factor authentication technique (i.e., a login name, a password, and verification through text message to a mobile phone), creates a more secure way for a person to read their test results online. This also goes for physician access.

Talley says he's managed to convince a number of vendors that it's in their interest to work with SEMHIE to prove that it's possible to validate identity on a standardized basis, that two-factor authentication and a single sign on approach can provide access to lab results by the patient, the doctor, and the insurance company.

"The reason you can stick your debit card into any ATM machine and get $100 regardless of the bank, or swipe your card at any point of sale is because 10 years ago institutions said that in collaboration with our vendors, this is the algorithm we're going to use and we want you to use it," Talley says. "If you don't want to use it, we'll bid you a tearful goodbye. Healthcare hasn't done that yet. But we're on the path."

Notes

[1] Harvard University. "Fact Sheet: Sugary Drink Supersizing and the Obesity Epidemic." June 2012.

[2] Dooling, Julie et al. "Survey: Patient Matching Problems Routine in Healthcare." *Journal of AHIMA* website. January 6, 2016.

Sign the MyHealthID Petition

https://petitions.whitehouse.gov

Starting March 20 HIM professionals and the general public are encouraged to take action for MyHealthID and sign the petition at https://petitions.whitehouse.gov. In order to receive a response from the Obama Administration, the petition must garner 100,000 signatures before April 19.

Reference

Harris Health System. "Harris County Hospital District Puts Patient Safety in the Palm of Your Hand." Press Release. April 5, 2011.

Mary Butler (mary.butler@ahima.org) is associate editor at the *Journal of AHIMA*.

Article citation:
Butler, Mary. "Finding John Doe: Patient Matching and the Need for a National Health Safety Identifier" *Journal of AHIMA* 87, no.3 (March 2016): 15-19.