National patient identifier advocates state their case

August 2021—*The iconic Timex slogan "It takes a licking and keeps on ticking" was designed to sell watches in the 1950s and '60s, but it could just as easily be applied to efforts to repeal the decades-long appropriations ban on a unique national patient identifier—year, after year, after year.*

Lack of a national strategy to address patient identification and matching has impeded adoption of digital health information technologies and poses consumer safety hazards, according to Patient ID Now, a coalition of industry stakeholders committed to advancing a national patient identifier program. Yet despite concerted advocacy efforts and proposed legislation seeking repeal of the ban—most recently advanced in July 2020 by congressional representatives concerned with collecting accurate patient information during the global pandemic—the U.S. Senate has upheld the ban in every federal budget since 1999.

The demand for transferring records among health care entities will continue to grow as health care networks merge and patients become increasingly mobile, exacerbating the potential for patient misidentification, says S. Joseph Sirintrapun, MD, director of pathology informatics at Memorial Sloan Kettering Cancer Center, New York City. "And I would hate to think that five years from today we're still discussing the NPI and nothing has been done."

CAP TODAY contributing editor Charna Albert asked five pathologists who support a unique national patient identifier why such a system is necessary, how it could be implemented, and what health care entities can do today to reduce the risk of patient misidentification. Here's what they had to say.

Has COVID changed the need for a national patient identifier or how such a program should be structured?

J. Mark Tuthill, MD, division head of pathology informatics at Henry Ford Health System, Detroit: COVID highlighted the fact that lack of a coherent and integrated patient identifier fragments the entire health care system. We saw this in Michigan, where we were initially sending a lot of SARS-CoV-2 testing out of our health system. Reintegrating that information so that we had appropriate records was a challenge, and that's a symptom of the fact that patient identification is left to each health care system to manage.

Dr. Sirintrapun

Dr. Sirintrapun (MSKCC): One issue that arose with COVID is we don't have a good way to track and properly identify patients. If a patient gets a test and then travels to another state and receives another test, it's probably counted as separate tests and separate people. How do we know all the tests that are run accurately reflect the number of cases? We have to do a lot of guesstimation. It potentially affects forecast modeling and the ability to develop public policy.

Brian R. Jackson, MD, medical director of support services, IT, and business development, ARUP Laboratories, Salt Lake City: COVID should be a wake-up call. One interesting thing about COVID has been all of the testing done in a nontraditional way, with specimen collection taking place outside health care facilities. From that perspective, patient identification has been a challenge. When I think about where we need to go in this country with medical diagnostics, something we need to improve upon is putting diagnostic testing closer to patients, with specimen collection in more convenient settings.

Cost, privacy threats, and fraud have been cited as reasons for not creating a national patient identifier program. Do any of these present potentially insurmountable obstacles?

Dr. Sirintrapun (MSKCC): The privacy and cost arguments are valid, but there are ways they can be overcome. First, you want to make the juice not worth the squeeze for hackers. The problem with Social Security numbers, and even electronic medical record numbers, is they are tied into systems that have value. Don't have the NPI tied into electronic medical record systems because those systems contain valuable information, such as whether patients have had cancer or have comorbidities that affect disability insurance. If you have an NPI that isn't tied, IT-wise, to these other things, the value diminishes. We have to provide modern infrastructure so that patients can be identified without having their NPI or other sensitive information exposed.

Estimates in some health care blogs have shown that the costs of implementing an NPI system could fall between $1 billion and $50 billion. Over time that can be mitigated. And the architecture doesn't need to be a complete overhaul of all our systems. But we know hospitals spend a lot of time and resources on identification, and if a mistake happens, costs are higher.

Dr. Tuthill

Dr. Tuthill (Henry Ford Health System): I think the obstacles are political. And certainly there have been significant privacy concerns at the grassroots level. But lack of an NPI is not preventing the government or insurance companies from accessing patient records. The challenge of integrating a patient's record across multiple episodes of care in different care environments affects patients and providers, and it is patients and providers who are most hurt by the lack of a patient identifier. In fact, a fragmented patient identifier probably enables fraud because it requires a lot of work to tell what medical care has been administered to a given patient over time and across medical institutions.

The cost of amalgamating patient records and reintegrating records across episodes of care has got to exceed the costs of implementing a national patient identifier. It took millions of dollars to deploy the national provider identifier program, but it saved billions of dollars in fraud and accounting and in the ease of monitoring physician and billing practices. I assume the same would be true at the patient level.

Dr. Jackson

Dr. Jackson (ARUP): The privacy threats to the way we manage health information have grown so rapidly—particularly with the advent of big data and the enormous volumes of personal information collected by the big tech giants—that in comparison, the theoretical privacy concerns of an NPI are becoming much less significant. It's technologically possible to use those data sets to reidentify just about any deidentified health care data if they were to get into the wrong hands. Given that, the privacy risk is the same whether or not we have an NPI.

I have trouble believing that cost concerns are a serious barrier because national governments excel at maintaining national identifier programs. If you look at the Census Bureau, for example, the federal government

has well-developed capabilities for acquiring, managing, and protecting data.

Sterling Bennett, MD, MS, senior medical director, pathology and laboratory medicine, and medical director, central laboratory, Intermountain Healthcare, Salt Lake City: I don't think any of these are insurmountable obstacles. The biggest hurdle is political, and privacy concerns are going to make the politics difficult. Large segments of the public are worried about their privacy or have underlying mistrust of the government and its use of any data. We've seen that Social Security numbers have been an avenue for identity theft and other invasions of privacy. An NPI would create potential for fraud, but people seem to be creative in that area already. I don't know that an NPI would materially change the likelihood of fraud occurring.

As for the costs, a national patient identifier would simplify the administrative aspects of the registration process, particularly if patients carried an NPI card. If we look at the total administrative cost associated with patient registration and with the attempts to match data in some efforts to share it across enterprises, I have a hard time believing the costs of maintaining the NPI would be greater than the savings associated with having an NPI.

What would you consider to be a worthwhile and realistic approach to a national patient identifier system?

Dr. Tuthill (Henry Ford Health System): There needs to be buy-in from the health care industry and support from physician groups such as the AMA. The identifier itself could be a sophisticated ID or digital certificate that would allow for greater monitoring. That would provide benefits not only in terms of sharing patient information among providers but in providing safety to consumers because patients would know when their identifier or insurance is being used fraudulently.

Dr. Sirintrapun (MSKCC): I advocate for a secure single centralized authentication system. The underpinning of such a system is a federated identity model, which would link a user's identity across multiple separate identity-management systems. Unique patient identifiers and other sensitive information would be housed locally within health systems and receive the same level of security and protection. Rather than exchanging the actual NPI during a data transfer, health care entities and the centralized authentication system would exchange tokens, which are simply pieces of data that stand in place of other, more valuable information, such as unique patient identifier metadata.

In other words, when a health system sends patient data to another system, the receiving organization would verify the patient's identity before the transaction can be completed, and the central authentication system would then complete a centralized verification confirming the identity of the patient whose data is being transferred. Thus, the patient's identity is securely validated across multiple separate health systems while alleviating the vulnerabilities of exchanging sensitive information among health systems. Encrypting the tokens creates another disincentive for hackers and adds an extra layer of security. Such a system would make hacking improbably hard, requiring penetration at many points.

Dr. Brodsky

Victor Brodsky, MD, associate professor and medical director of information systems, Washington University School of Medicine, St. Louis: Informed consent is central to the current standard of care and should therefore become the cornerstone of health information exchange. Mechanisms used by two-factor authentication to obtain permission have matured and are ubiquitously accessible via phone calls, text messages, and emails. A responsive, highly available infrastructure can enable time-limited renewable health care data transmission consent that can be automatically requested, obtained, and documented for a given institution, provider, diagnosis, or dependent,

either on the fly or prior to an appointment. Such an approach is of paramount importance since the database software used by the current generation of health care applications is inherently insecure. Without requiring permission from the patient to transmit data, a single malicious intrusion, outdated misconfiguration, or accidental data leak in any of the multiple medical offices employing the NPI could result in the entirety of the interconnected data set for a given patient—or millions of them—being permanently exposed.

What measures do you recommend that hospitals or health care systems take, beyond what's routine or government mandated, in the absence of a national patient identifier?

Dr. Tuthill (Henry Ford Health System): Master patient indexing technology is critical and not widely deployed. Some of the more advanced medical record systems use it, but how often do we go through and look at our patient records to see if there are mismatches? At the level of the laboratory information system, the technology is not well deployed. We need to use it to surveil our systems to determine how many duplicate patient records are being created. When we sanitize patient databases, we find significant levels of patient misidentification. Sanitizing is a fair amount of work at the level of millions of records, but at the level of billions of records it's an almost insurmountable task. As time goes forward, more and more records are created and integrating those records becomes very challenging. Getting on the train sooner rather than later is important. On the flip side, the ability to reintegrate records at the meta level has become easier as computers have gotten faster and we're able to crunch through records and create indexes that reconnect patients across different systems. But it's at a significant computing cost, and it's misplaced. We're wasting resources by not doing things the right way.

Dr. Bennett

Dr. Bennett (Intermountain): The first step is to create an internal master patient index. The second step is to make the patient ID accessible to patients. In many cases, a health system will have a master patient index number or medical record number but the patient doesn't know it or need to provide it. I'm aware of health systems that issue an ID card with the MRN to patients, and patients are expected to present their ID card. So the third step is for health care systems to require the patient to provide that ID number at the time of service. The fourth step is when health care entities request services from other health care entities, the referring entity must provide the patient's ID number. That number would be returned with the data so the information could be linked back to the correct patient. This would be a way to identify the patient for the referring entity in the absence of an ID number that is transferable across all systems.

Dr. Sirintrapun (MSKCC): Let's at least talk about standardizing demographic information and the data pieces health care entities incorporate into their patient identification algorithm or procedures. Every hospital does it differently.

Dr. Brodsky (Washington University School of Medicine): We don't have to wait for government regulations to begin automatically notifying patients of inbound or outbound data transmissions. Obtaining consent for data sharing via the patient portal would be an appropriate step for patients and would potentially prepare institutions to adopt a more centralized type of system that would inform patients their data are being transmitted and obtain and document their consent. These are measures that don't have to wait for the national patient identifier or legislation.