Advancing a Nationwide Patient Matching Strategy

By Rita Torkzadeh, MS; Ben Moscovitch, MA; Josh Rising, MD; Jitin Asnaani, MBA; Michelle De Mooy, MA; Jamie Ferguson, BS; Mark Gingrich, MS; Shaun Grannis, MD; Eric Heflin, BS; Andrew Hohwald, MBA; Aaron Miri, MBA; Robert S. Rudin, PhD; Catherine Schulten, BS; Allison Viola, MBA, RHIA; Chantal Worzala, PhD; and John Halamka, MD

Accurately linking people with information about them that is stored across various systems is common to many life activities—such as when qualifying for a loan or registering to vote. While all industries don't always get data matching right, this problem can be particularly challenging in healthcare. One example of the problem can be seen at a single Houston health system, which reported it has 2,488 records with the patient name Maria Garcia, of which 231 Maria Garcias share the same birth date.[1,2] Some of these records are likely duplicates, but how many and which ones?

One in five hospital chief information officers report that ineffectively linking people to their records—called matching—led to at least one case of patient harm in the prior year.[3] Another study found that the cost of fixing each incorrectly merged record can exceed $1,200.[4]

Better matching would help organizations more effectively exchange data and give patients and clinicians more accurate information, as well as reduce costs by preventing duplicate tests and support more robust research using real world data.

Match rates vary widely. Facilities within the United States can achieve match rates of 90 percent or higher when the organization maintains high data quality and uses the same version of a health record system.[5] On the other end of the spectrum, at some facilities up to 20 percent of patient records are not accurately matched within a healthcare system,[6,7,8] and error rates can approach 50 percent when sharing across facilities, though significant variation exists among organizations and technologies.[9]

Matching issues arise when records for the same patient are not linked, resulting in inaccurate record creation, or when records for different individuals are inadvertently merged—a far rarer occurrence. These errors can originate during patient registration for an appointment, or when exchanging data among facilities. Demographic data derived from electronic health records are commonly used to match patients. Some organizations rely on unique identifiers—such as numbers or biometrics (like palm scans)—to locate patient records. Many healthcare systems outside the United States use national identifiers, though Congress to-date has prohibited the use of funds for such an approach domestically due to concerns around privacy and government regulation.

Improving patient matching has garnered widespread public and private sector interest.[10,11] The Government Accountability Office, responding to a bipartisan request from Congress, is studying approaches to matching.[12] The Office of the National Coordinator for Health Information Technology (ONC) launched a contest to evaluate different matching algorithms.[13] And the College of Healthcare Information Management Executives (CHIME) sponsored a patient identification competition.[14] The ONC competition used a database containing synthetic data to compare the effectiveness of different algorithms and the three winners all required some amount of manual review to adjudicate complicated linkages. While CHIME selected four finalists in its competition, the organization suspended the competition late last year after concluding that the goals were not met.[15]

These independent activities—and because different technologies are used in healthcare for identification and matching—could be strengthened with a coordinated strategy to ensure effective matching across organizations. To advance such a strategy, in 2017, The Pew Charitable Trusts and Dr. John Halamka, MD, chief information officer of the Beth Israel Deaconess Medical Center and a professor at Harvard Medical School, convened approximately two dozen patient matching experts from government, technology vendors, healthcare systems, and other organizations. The group, many of whom are authors of this article, sought to identify key characteristics that a nationwide matching strategy should embody. The group did not intend to promote a single technology or generate consensus, but rather to hear different perspectives from competitors in

the marketplace. This article summarizes the characteristics identified by this group, and outlines actions the public and private sectors can take to advance a nationwide strategy for improved patient matching.

Characteristics Recommended for Improving Patient Matching

A nationwide strategy to improve patient matching should include several key elements, including its governance, design, and value provided.

Governance and Policy

A nationwide approach to patient matching would address the disparate and conflicting methods used to identify and match patients to their health information, including demographics, biometrics, and other credentials. For example, healthcare organizations that implement different biometrics (e.g. one facility uses palm veins and another iris scans) may not be able to use them for matching between different facilities. A coordinating entity that establishes best practices and points to standards could address several challenges—such as how to depict different biometrics. This coordinating entity should have the following characteristics:

- **Trusted organization:** A neutral coordinating organization with balanced stakeholder representation that is dedicated to improving care quality and coordination should manage the development, policies, and evolution of a nationwide strategy. This organization would identify needed policies, ensure that solutions complement one another, and assess whether approaches are overly burdensome to resource-constrained organizations—such as critical access hospitals. This organization should maintain policies for patient identification, support improved data quality, establish criteria for solutions, develop rules, and identify standards that technology developers and hospitals would agree to follow. In effect, this trusted entity would establish a standards-based infrastructure to improve patient matching. This entity should focus on technology-neutral approaches in the absence of a critical mass of support for a single solution.
- **Private sector-led:** The private sector should lead the strategy, with government supporting—but not directing—efforts because providers and technology developers will bear primary responsibility and implementation costs. Meanwhile, federal and state governments could enact policies to support recommendations, such as incentives for adherence to standards.
- **Universal data exchange policy:** Currently, healthcare organizations often enter into data sharing agreements with each information exchange partner, which can be costly and time-consuming.[16] Creating a universal policy supported by a trusted entity would define how and what data can be used for matching, and set privacy rules and other appropriate policies salient to matching. Such a universal agreement could function as an authoritative reference or implementation guide that could be leveraged and adopted by hospitals and organizations that facilitate information exchange—such as the CommonWell Health Alliance, a not-for-profit association of health information technology companies building a data exchange network, and the Sequoia Project's Carequality, a public-private collaborative that relies on consensus-based processes for inter-network interoperability.
- **Transparency and trust:** The success of a nationwide strategy relies on ubiquitous implementation by healthcare organizations and acceptance by patients. To achieve large-scale buy-in, the components of a nationwide strategy should be publicly disclosed. Earning that support must also include ongoing input from patients, providers, technology developers, and others.
- **Clarification across states:** States may also implement privacy and data exchange policies differently, as federal regulations only establish minimum requirements that some states expand upon.[17] Clarifications and consistent application of data sharing practices across states could facilitate organizations' willingness to implement a nationwide strategy. The trusted entity could help harmonize state policies and address variations.

Design, Architecture, and Privacy

As the technological capabilities of organizations vary widely, a nationwide matching strategy should both establish minimum criteria that should be met while also providing guidelines for further infrastructure development. The architecture should protect sensitive patient data—such as on substance use—and foster the ability for patients to know who accessed their files and act on their data sharing preferences where required by federal or state laws.[18] The strategy should also have the following characteristics:

- **Flexibility:** The framework for a nationwide strategy should support different technologies and solutions that can work together to improve matching to the greatest extent possible. The trusted entity could help build an infrastructure that allows seemingly incompatible solutions—such as different biometrics—to be used more effectively for matching. Some healthcare facilities may be able to easily modify how they conduct patient matching, while others may not. As over half of hospitals use more than one matching method,[19] support for a heterogeneous mix of technologies is needed to accommodate variation. Over time, a preferred technology solution may emerge and could be adopted if it has a critical mass of support.
- **Trusted identities:** Improving patient matching relies on each healthcare organization correctly identifying patients. Authenticating that individuals are who they say they are—including through the use of multi-factor authentication such as confirming registration via email or using smartphones—can help improve identification. Organizations should follow generally accepted approaches—such as those from the National Institute for Standards and Technology or the National Strategy for Trusted Identities in Cyberspace—for accurately identifying individuals and securing those identities.[20]
- **Standards:** Health information technology developers and healthcare facilities should support and implement agreed-upon standards—such as a minimum demographic data set or support for standards identified previously by Integrating the Healthcare Enterprise or federal advisory committees. This may include government involvement to set and enforce standards, especially until the establishment of a trusted entity that can oversee the development of a standards-based infrastructure. Optionality within these standards should be constrained to the greatest degree possible without impeding innovation.
- **Error resolution:** Healthcare organizations may not easily identify when records are incorrectly matched. A nationwide matching strategy should enable patients to attest to the veracity of the information contained in a record and correct any matching errors, and support cross-organization sharing of corrections when mistakes are found in the absence of patient involvement.
- **Patient empowerment and choice:** Because individuals have different preferences regarding with whom and for what purposes their information is shared, systems should support this. Patients should be encouraged to speak with their healthcare providers to understand the benefits and drawbacks of sharing data, and when exchanging information can legally occur among providers absent explicit consent. Additionally, patient data collected for matching and identification purposes should not be shared with third parties for non-treatment purposes without their authorization. For example, some patients may want their medical data merged with grocery store purchases to better characterize their overall health, while others may not.

Value to Stakeholders

While implementing a nationwide strategy to improve patient matching can improve care quality and reduce costs, it may also introduce additional risks and costs. Some things to keep in mind include:

- **Return on investment:** The benefits accrued by organizations and patients must exceed the risks, especially for organizations that bear the greatest implementation costs. Both market forces and government policies can create those benefits—such as through cost reductions from duplicate records, higher care quality, the ability to participate more effectively in data exchange networks, and other potential drivers.
- **Benefits accrue early:** The full benefits may not accrue until a critical mass of facilities participates. Organizations that consider investing early may question whether other organizations will also implement a nationwide strategy. A nationwide strategy should enable early adopters to realize improvements immediately to encourage adoption.
- **Legal safeguards:** Improved patient matching may also expose healthcare organizations to increased liability if data are illegally accessed or unintentionally disclosed. These consequences may occur even when organizations follow best practices and standards and comply with regulations. Legal protections—such as safe harbors—may be needed to shield healthcare providers, technology developers, and other organizations who act in good faith.

Barriers and Recommended Next Steps

A successful nationwide strategy for improved patient matching faces multiple barriers and requires collaboration among the public and private sectors.

First, no single organization currently has the responsibility to improve matching on a nationwide scale. Healthcare providers and technology developers should agree on the need for a trusted entity to develop a common infrastructure, establish governance policies, identify a business model, and commit to following the standards and guidance provided by this organization. This entity—whether identified among existing groups or created anew—may also require seed funding and assistance in launching these activities.

Second, government agencies should consider policies to advance a nationwide strategy. ONC could update its certification criteria to add minimum data sets or other best practices, evaluate how to measure matching between facilities, and foster development of a universal data sharing agreement (which ONC is expected to release this year[21]). The Centers for Medicare and Medicaid Services could consider revising its policies, such as by amending its conditions of participation, working with the Joint Commission on adding patient matching practices to hospital accreditation, or developing other regulatory clarifications needed to assuage concerns about sharing data. Given that Congress has prevented the federal government from establishing a national patient identifier, lawmakers should assess whether additional clarifications are needed for agencies to support a nationwide strategy. State governments can also clarify or harmonize privacy policies that inhibit matching or data exchange.

Finally, legal and cultural challenges must be considered. Some organizations may fear liability when sharing data or resist increased patient control. And some individuals may be uncomfortable using biometrics or other technologies, or they may be concerned about the security of medical information used for matching. Congress should assess whether the implementation of a nationwide strategy would benefit from appropriate clarifications, work with the private sector in enacting policies, and evaluate the need for additional safeguards to protect privacy while still ensuring that medically appropriate data can be communicated.

By enacting a nationwide strategy that embodies these characteristics, hospitals, technology developers, and the broader healthcare ecosystem can tackle one of medicine's greatest challenges: the ability to better link patients to their records to improve care coordination and reduce costs.

Notes

1. Lippi, Giuseppe et al. "Patient and Sample Identification. Out of the Maze?" *Journal of Medical Biochemistry* 36, no. 2 (April 22, 2017): 107-112. https://doi.org/10.1515/jomb-2017-0003.
2. Harris Health System. "Harris County Hospital District Puts Patient Safety in the Palm of Your Hand." www.prlog.org/11430165-harris-county-hospital-district-puts-patient-safety-in-the-palm-of-your-hand.html.
3. College of Healthcare Information Management Executives. "Summary of CHIME Survey on Patient Data-Matching." May 16, 2012. https://chimecentral.org/wp-content/uploads/2014/11/Summary_of_CHIME_Survey_on_Patient_Data.pdf.
4. Morris, Genevieve et al. "Patient Identification and Matching Final Report." Office of the National Coordinator for Health IT. February 7, 2014. www.healthit.gov/sites/default/files/patient_identification_matching_final_report.pdf.
5. Ibid.
6. Bipartisan Policy Center. "Challenges and Strategies for Accurately Matching Patients to Their Health Data." June 2012. http://cdn.bipartisanpolicy.org/wp-content/uploads/sites/default/files/BPC%20HIT%20Issue%20Brief%20on%20Patient%20Matching.pdf.
7. College of Healthcare Information Management Executives. "Summary of CHIME Survey on Patient Data-Matching."
8. The Pew Charitable Trusts. "Patient Matching Errors Risk Safety Issues, Raise Health Care Costs." June 29, 2017. www.pewtrusts.org/en/multimedia/data-visualizations/2017/patient-matching-errors-risk-safety-issues-raise-health-care-costs.
9. Morris, Genevieve et al. "Patient Identification and Matching Final Report."
10. Letter from US Senators Elizabeth Warren, Orrin Hatch, Sheldon Whitehouse, Tammy Baldwin, and Bill Cassidy to Gene L. Dodaro, Comptroller General, US Government Accountability Office. October 3, 2017. www.warren.senate.gov/files/documents/2017_10_03_GAO_Patient_Matching_Letter.pdf.
11. 115th US Congress. "Departments of Labor, Health and Human Services, and Education, and Related Agencies Appropriations Bill, 2018." US Committee on Appropriations. https://appropriations.house.gov/uploadedfiles/23920.pdf.
12. 114th US Congress. "21st Century Cures Act (Public Law 114–255)." December 13, 2016. www.congress.gov/114/plaws/publ255/PLAW-114publ255.pdf.

13. Department of Health and Human Services. "Office of the National Coordinator for Health Information Technology Announcement of Requirements and Registration for 'Patient Matching Algorithm Challenge.'" April 28, 2017. www.patientmatchingchallenge.com/sites/default/files/3608_001.pdf.
14. HeroX. "CHIME National Patient ID Challenge." https://herox.com/PatientIDChallenge.
15. College of Healthcare Information Management Executives. "CHIME National Patient ID Challenge." https://chimecentral.org/chime-npidchallenge/.
16. Office of the National Coordinator for Health IT. "Trusted Exchange Framework Public Comments." August 2017. www.healthit.gov/sites/default/files/tefca_public_comments_as_of_2017_08_28_final_xlsx.xlsx.
17. Johnson, Kate et al. "Getting the Right Information to the Right Health Care Providers at the Right Time: A Road Map for States to Improve Health Information Flow Between Providers." National Governors Association. 2016. www.nga.org/files/live/sites/NGA/files/pdf/2016/1612HealthCareRightInformation.pdf.
18. US Department of Health and Human Services, Office of the Secretary. "42 CFR Part 2. Confidentiality of Substance Use Disorder Patient Records." January 18, 2017. www.regulations.gov/document?D=HHS-OS-2016-0005-0377 and www.ecfr.gov/cgi-bin/text-idx?c=ecfr&sid=b7e8d29be4a2b815c404988e29c06a3e&rgn=div5&view=text&node=42:1.0.1.1.2&idno=42.
19. College of Healthcare Information Management Executives. "Summary of CHIME Survey on Patient Data-Matching."
20. Grassi, Paul A., Michael E. Garcia, and James L. Fenton. "Digital Identity Guidelines." National Institute of Standards and Technology. June 2017. https://doi.org/10.6028/NIST.SP.800-63-3.
21. Office of the National Coordinator for Health Information Technology. "Draft Trusted Exchange Framework." January 5, 2018. www.healthit.gov/sites/default/files/draft-trusted-exchange-framework.pdf.

Rita Torkzadeh (rtorkzadeh@pewtrusts.org) is officer, health information technology; Ben Moscovitch is manager, health information technology; and Josh Rising is director, healthcare programs at The Pew Charitable Trusts. Jitin Asnaani is executive director at CommonWell Health Alliance. Michelle De Mooy is director of the Privacy and Data Project at the Center for Democracy and Technology. Jamie Ferguson is vice president, health IT strategy and policy at Kaiser Permanente. Mark Gingrich is chief information officer at Surescripts. Shaun Grannis is director of the Regenstrief Center for Biomedical Informatics and associate professor at the Indiana University School of Medicine. Eric Heflin is chief technology officer at The Sequoia Project and HIETexas. Andrew Hohwald is senior data analyst, clinical services group at HCA Healthcare. Aaron Miri is former chief information officer and vice president, government relations at Imprivata. Robert S. Rudin is information scientist at RAND Health, RAND Corporation. Catherine Schulten is vice president, product management at LifemedID. Allison Viola is director, health IT policy at Kaiser Permanente. Chantal Worzala is vice president of health information and policy operations at the American Hospital Association. John Halamka is chief information officer at Beth Israel Deaconess Medical Center.

Article citation:
Torkzadeh, Rita. "Advancing a Nationwide Patient Matching Strategy." *Journal of AHIMA* 89, no. 7 (July-August 2018): 30-35.