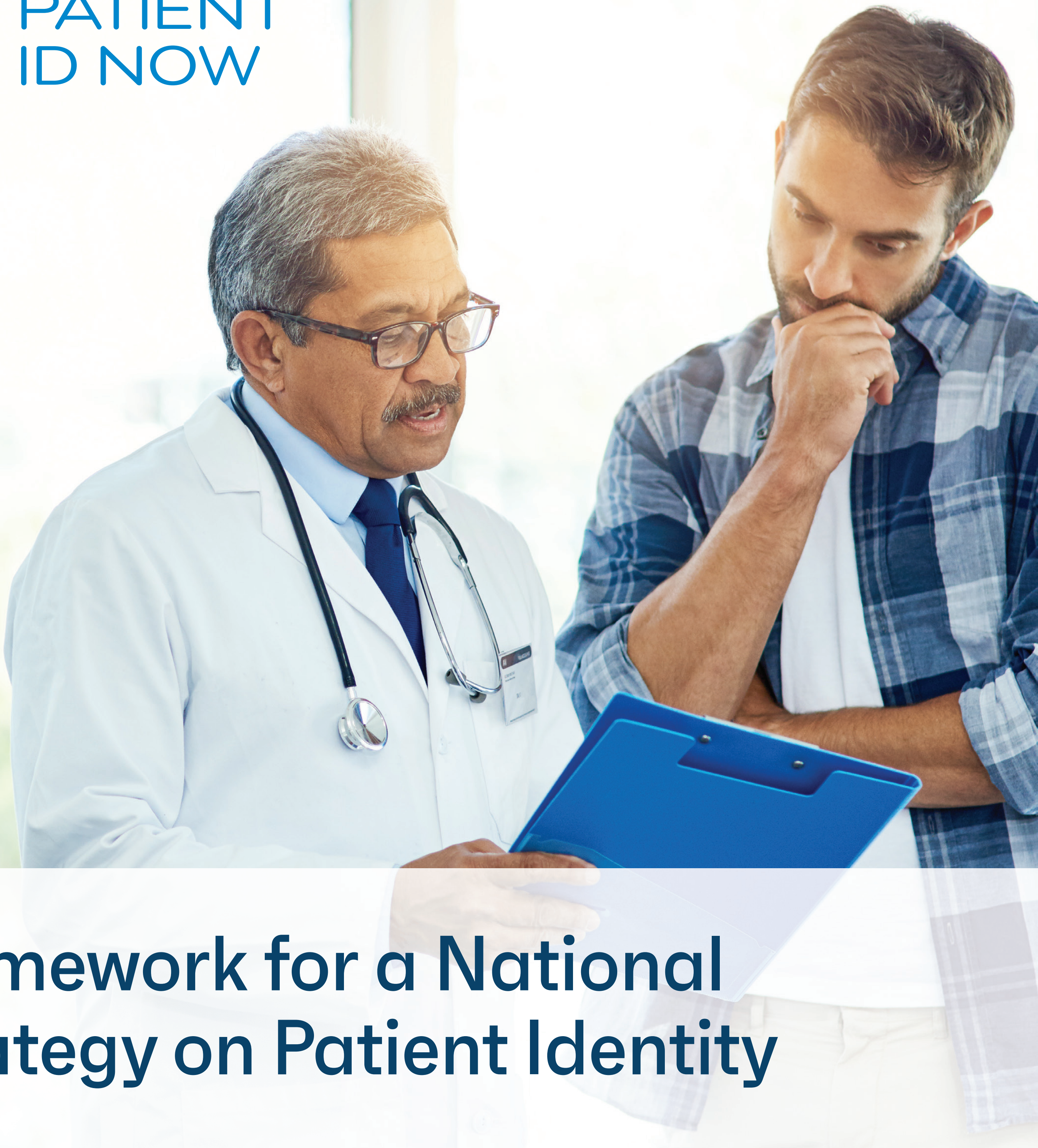
PATIENT
ID NOW



Framework for a National Strategy on Patient Identity

A Proposed Blueprint to Improve Identification and Matching

About Patient ID Now

Patient ID Now is a coalition of healthcare organizations representing a wide range of healthcare stakeholders committed to advancing through legislation and regulations a nationwide strategy to address patient identification.

Introduction

Since passage of the *Health Information Technology for Economic and Clinical Health (HITECH) Act* in 2009, the digitization of health information has rapidly accelerated, with electronic health records (EHRs) and electronic charts finally replacing the paper charts and records of prior decades in countless care settings across the country. As healthcare enters an increasingly electronic and interoperable ecosystem, ensuring the highest quality of patient electronic health information and data is fundamental to health and healthcare, including clinical and public health. Health information must be accurate, timely, clinically robust, and complete to inform safe, reliable, and appropriate clinical care decisions for every patient. To meet these standards, a critical matter must be addressed in healthcare: the issue of patient identification and matching.

The ability to consistently and reliably identify and match patients to their health information is vital as they seek care across the continuum. Data integrity, including patient identification, is essential to advance interoperability and support the access, exchange, and use of electronic health information. Yet, inaccurate, incomplete, or inconsistently formatted demographic information in patients' records have been shown to cause major adverse patient outcomes, including death.[1] Meanwhile, the amount of information collected about individuals both in and out of the clinical setting increases without solving the issue of identification and matching, and potentially at the expense of privacy and data protection.

Challenges and Consequences

The lack of a national strategy around patient identification and matching has limited the progress in the adoption of digital health information technologies and management. It also threatens the continued advancement of digital health and virtual care. Meanwhile, the challenges and consequences from incorrectly identifying and matching patients to their health information are amplified by the ever-increasing exchange of health information across the healthcare system.

Quality of Care and Patient Safety

Today, there is no consistent and accurate way to link patients to their health information as they seek care across the continuum in the United States. Countless times every day, a patient record is mismatched or is duplicated in multiple disparate records. Medications are prescribed for patients lacking a complete medical history in their record; allergies are missed, diagnoses are lost or delayed, and duplicative tests are ordered. The problem of patient misidentification is so dire that one of the nation's leading patient safety organizations, the ECRI Institute, named patient misidentification among the top ten threats to public safety.[2] Clinicians and medical personnel across the spectrum must be able to trust that patient records they are using to make vital care decisions are complete and accurate.

Financial Implications

The issue of patient misidentification creates additional financial burdens to patients, clinicians, and institutions. A 2018 Black Book market research survey found that the expense of repeated medical care due to patient misidentification costs an average of $1,950 per inpatient stay and over $800 per emergency department visit.[3] According to a study of healthcare executives, misidentification costs the average healthcare facility $17.4 million per year in denied claims and potential lost revenue.[4] The Black Book survey also indicates that denied claims as a result of patient misidentification costs the US healthcare system over $6 billion annually.

Public Health Impediments

Now, more than ever, the COVID-19 pandemic highlights the need to address patient identification and matching. Accurate identification of patients is one of the most difficult operational issues during a public health emergency, including the collection of patient demographic information (e.g., name, address, phone number) and the implementation of a method to ensure that the information remains attached to the patient. Field hospitals, temporary testing sites, and vaccination sites in parks, convention centers, and parking lots exacerbate these challenges. Collecting limited demographics in mass vaccination settings creates challenges for immunization information systems (IIS), which aim to consolidate immunization records for individuals across the lifespan, and to share them back with patients' medical records.

The fact that most COVID-19 vaccines are currently administered in two doses increases the risk to improperly attributing vaccine status to patients. It also adds to the difficulties of correct attribution to patient identification, such as ensuring brand consistency between dose one and dose two. Patient ID Now coalition members have received reports of vaccination registrations causing thousands of duplicate records within a single system, costing some hospitals and health systems at least $12,000 per day to rectify these errors. There are also reports of some vaccination sites being denied additional vaccines because patient record systems incorrectly show patients as not having received previously administered vaccinations. Ensuring the correct patient medical history is accurately matched to the patient is critical for future patient care, claims billing, patients' long-term access to their complete health record, and for tracking the short-term and long-term effects of COVID-19.

Privacy Concerns

The lack of a national strategy around patient identification and matching also presents several troubling privacy issues for patients. Right now, the healthcare ecosystem faces an "inverse" privacy problem –individuals must repeatedly disclose a significant amount of individually identifiable information to each healthcare provider they see in an attempt to achieve an accurate match of the patient to their medical record. Furthermore, payers often maintain separate proprietary identifiers for patients, increasing the number of identifiers in use.

Even more worrying for patient privacy is risk of overlays—i.e.,–the merging of multiple patients' data into one medical record, causing a patient to have access to other patients' health information, which could result in an unauthorized disclosure under the *Health Insurance Portability and Accountability Act (HIPAA)*, or even worse, a patient receiving treatment for another patient's disease.

Public Policy Compliance

Federal legislation, such as the *Health Information Technology for Economic and Clinical Health (HITECH)* Act, the *American Recovery and Reinvestment Act of 2009 (ARRA)*, and the 21st Century Cures Act requires federal agencies, including the Centers for Medicare and Medicaid Services (CMS) and the Office of the National Coordinator for Health Information Technology (ONC), to promulgate rules to operationalize data sharing, exchange, and interoperability. Failure to share data effectively may implicate allegations of information blocking, penalties, and other consequences. The need to resolve patient identification and matching issues is essential to moving toward nationwide interoperability.

History

Efforts to address patient identification and matching and the resolve to advance a national strategy are not new, but have been hampered for more than two decades by the inclusion of Section 510 within the Labor, Health and Human Services, Education, and Related Agencies Appropriations bill within the federal budget. This section states that "None of the funds…may be used to promulgate or adopt any final standard…providing for, or providing for the assignment of, a unique health identifier for an individual." The language was originally included because of patient privacy concerns. However, in the years since, the full implementation of HIPAA to address patient privacy, the increased use of electronic health records (EHRs), and the push for increased interoperability within the US healthcare system means that it is time to move past the previous barriers. It is critical to support the US Department of Health and Human Services' (HHS) ability to work with the private sector to create a national strategy around patient identification and matching. Years of historical work can be leveraged in the development of a national strategy. Examples include:

- In 1995, ASTM International published "E1714, a Standard Guide for Properties of a Universal Healthcare Identifier (UHID)," which was updated in 2007.[5]
- In 2008, the RAND Corporation published a study entitled, "Identity Crisis: An Examination of the Costs and Benefits of a Unique Patient Identifier for the U.S. Health Care System."[6]
- In 2010, the President's Council of Advisors on Science and Technology (PCAST) issued recommendations about how to take better advantage of health information technology to increase healthcare quality while reducing costs.[7]
- In January 2012, the Bipartisan Policy Center (BPC) issued a report entitled, "Challenges and Strategies for Accurately Matching Patients to Their Health Data."[8]
- In 2014, ONC released a report building on existing patient matching strategy work of ONC, which included an environmental scan to assess the current industry capabilities and best practices for patient identification and matching.[9]
- In 2016, the *21st Century Cures Act* directed the US General Accountability Office (GAO) to "review the policies and activities of the Office of the National Coordinator for Health Information Technology and other relevant stakeholders…to ensure appropriate patient matching to protect patient privacy and security with respect to electronic health records and the exchange of electronic health information."[10]
- In 2016, the Sequoia Project released a "Framework for Cross-Organizational Patient Identity Matching" which included a patient matching maturity model and minimally acceptable patient matching practices designed to help organizations improve patient matching across organizational boundaries. This framework was updated in 2018.
- In 2017, ONC held a "Patient Matching Algorithm Challenge," designed to "bring about greater transparency and data on the performance of existing patient matching algorithms," and to "spur the adoption of performance metrics for patient data matching algorithm vendors," in which 140 teams sent in over 7,000 submissions.
- In 2018 the RAND Corporation published "Defining and Evaluating Patient-Empowered Approaches to Improving Record Matching." This study evaluated ten existing and proposed approaches to patient identification against 11 evaluation criteria.[11]
- In 2018, the Pew Charitable Trusts released a study entitled, "Enhanced Patient Matching is Critical to Achieving Full Promise of Digital Health Records."[12]
- In 2018, ONC developed and released the *Patient Identification SAFER Guide*, which includes recommended safety practices associated with the reliable identification of patients in the EHR.
- In 2019, the GAO released a report required in the *21st Century Cures Act*, outlining the challenges of patient identification and exploring potential solutions to patient matching.
- In December 2019, a Congressional Appropriations Agreement for FY 2020 directed ONC, along with other pertinent Federal agencies, to "provide a report…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."[15]
- In January 2020, ONC's Annual Meeting held panels exploring patient identity, including sessions entitled "Unique Perspectives on Unique Patient IDs"[16] and "Congressional Perspective on Unique Patient IDs." ONC also held a Patient Identity and matching Working Session in June 2020.
- In 2020, the American Health Information Management Association released a white paper entitled, "A Realistic Approach to Achieving a 1% Duplicate Record Error Rate."[17]

- In December 2020, ONC announced Project US@, an initiative in collaboration with Health Level 7 (HL7), the National Council for Prescription Drug Programs (NCPDP), and X12 (along with the other standards development organizations (SDOs) and members of the Health Standards Collaborative (HSC)), to develop a unified specification for address in health care.[18]

Common themes emerge from the work done over the past decade on patient identification and matching, including: 1) the likelihood that there will not be one single solution, but rather a combination of solutions included within a national strategy; 2) the need to develop short- and long-term objectives and goals; 3) the need for diversity in innovation and approaches; 4) the need to consider technical, technological, legal, policy, economic, social, and political implications and ramifications; 5) the essential nature of privacy and security considerations, and; 6) the benefits of public-private sector collaboration.

A National Strategy to Improve Patient Identity

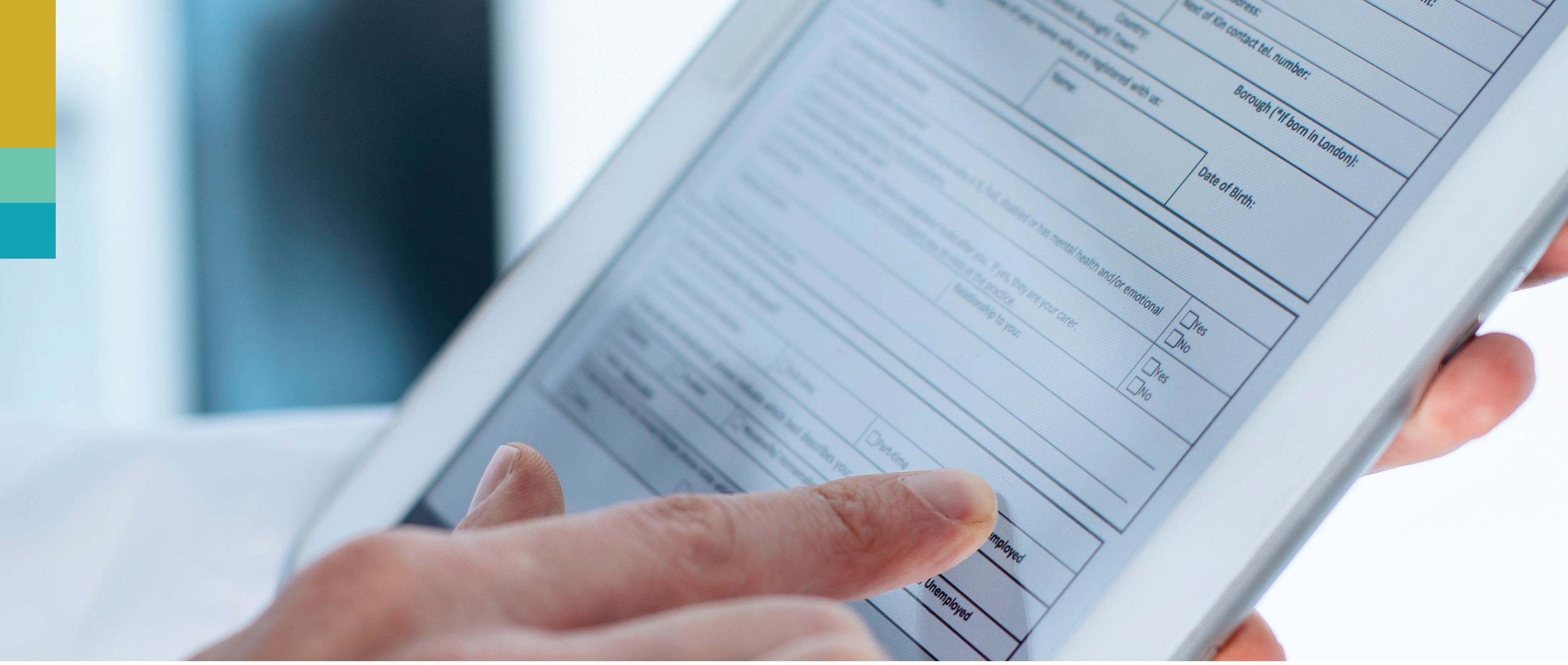
Federal leadership and action, along with collaboration with the private sector and public health, is necessary to create and deploy a national strategy around patient identification and matching. In January 2021, the Patient ID Now coalition created a work group consisting of member organizations within the coalition representing the breadth of the healthcare sector, including organizations representing patients, physicians, providers, health information professionals, health information technology companies, and public health to create a framework for a national strategy around patient identity. The work group met over several weeks to develop the framework, and input was provided by the broader coalition membership. **The Patient ID Now coalition offers the following framework to inform the creation of a national strategy.**

To help ensure a timely and comprehensive approach, the federal government should closely collaborate with the private sector and with state, local, tribal and territorial public health authorities. Leveraging findings and recommendations from prior public and private sector initiatives, we describe foundational components of and considerations for a National Strategy to Improve Patient Identity.

Accurate Identification and Match Rates

Eliminating matching errors is the primary goal of a national strategy around patient identification and matching. A national strategy to address patient identification and matching should:

1. **Improve matching rates across multiple scenarios to minimize errors, including addressing duplicates, overlays, and overlaps.** A duplicate record is created when two or more medical numbers or site-specific identifiers are created for the same person, causing them to have two or more records.[19] An overlay occurs when the incorrect patient is registered, admitted, or documented on another patient's record.[20] Inappropriate merges may also occur when different individuals are incorrectly identified as duplicates and inappropriately merged into a single record. An


Next of Kin contact tel. number:
Borough (*if born in London):
Date of Birth:
Yes
No
Yes
No
Part-time
Employed
Unemployed

overlap occurs when there is more than one unique patient identifier (UPI) for the same person across two or more facilities in the enterprise and may result in the creation of duplicate records.[21]

2. **Provide guidance on the process of matching and identity resolution.** While there may be various methods of matching patient records, guidance should be provided for the processes as a baseline.
3. **Provide guidance, including benchmarks and standards, as to how error rates are calculated across health IT systems and organizations.** Error rates can differ depending on how an organization's technology and methodology calculate it. While some technologies offer quality and benchmarking reports to manage the Master Patient Index (MPI)/ Enterprise Master Patient Index (EMPI), others do not. The same holds true for calculating duplicate error and creation rates.[22]
4. **Identify performance measures, such as minimum acceptable levels of accuracy.** The strategy for patient identification and matching should include attainable levels of accuracy with a goal of 100%. A national strategy should also consider the public reporting of minimal levels of accuracy.
5. **Align with guidelines provided by the National Institute of Standards and Technology (NIST).** A national strategy should leverage the work already underway by the federal government, including the privacy, security, and digital identity guidelines developed by NIST.
6. **Develop, disseminate, and conduct training on patient identification and matching, and encourage testing, evaluation, and optimization when appropriate.** This includes training for those who are involved in the implementation of a national strategy, such as providers, health information professionals, data integrity specialists, payers, public health organizations, health information exchanges, and health IT organizations.

Privacy

Privacy is a bedrock for the protection of health information and has been prioritized within the health system over the last two decades with the implementation of HIPAA. Any national strategy around patient identification and matching should continue and build upon the privacy protections found in HIPAA. A national strategy to address patient identification and matching should:

1. **Leverage public and private sector resources to help address patient privacy issues**. In addition to OCR and NIST materials and guidance, the national strategy can look to resources such as the principles of Self-Sovereign Identity (SSI),[23] and Privacy by Design.[24]
2. **Consider ways to advance the ability of patients to invoke more granular consent, while still adhering to the HIPAA minimum necessary requirement[25] as a floor.** Patient consent regarding privacy is paramount. Alternate ways of handling consent should be explored, including patient decisions on their data at a more granular level to limit unnecessary or inappropriate access to, and disclosure of, information concerning the patient's identity. At the same time, at a minimum, stakeholders should adhere to the minimum necessary requirement for payment and healthcare operations.

3. **Allow patient privacy preferences to evolve.** A patient's privacy preferences may evolve as their clinical situation changes. The strategy should enable changes to be made easily, quickly, and at no cost to the patient. This includes respecting patients' abilities to determine access to their identifiable information.
4. **Improve the ability of patients to easily understand their privacy options.** Patients should be able to understand how to simply manage their privacy preferences and consent to share their PHI.
5. **Support anonymity when appropriate.** The strategy should support prohibitions against re-identification of de-identified PHI.
6. **Not require a federal-level centralized database of Personally Identifiable Information (PII).** The strategy should be supported by a decentralized architecture and should avoid the need for a centralized database of patient identifiable information.
7. **Be limited to healthcare identification-related purposes.** A patient identification strategy should not be used for any purpose other than to connect a patient to their health information.
8. **Safeguard patient data, including for public health and research use cases.** Public health and research must also safeguard patient privacy, including ensuring only authorized users access identified data and promoting appropriate data minimization and retention policies.
9. **Support the ability to restore a patient's privacy if a violation has occurred.** In cases including data breach or identity theft, the ability to protect and restore a patient's compromised PII should be considered and addressed.
10. **Safeguard patients' identity when health information is shared amongst providers in line with requirements from current information blocking rules.** Care increasingly involves the use of data across multiple systems and/or providers, and patient privacy preferences related to identity in these instances should still be considered.

Security

Patients must be assured that not only is information related to their identity is kept private, but it is secure. A national strategy around patient identification and matching should:

1. **Support each principle of the CIA triad (confidentiality, integrity, availability) at the highest level possible without sacrificing patient safety.** A strategy must support organizations' ability to keep data confidential, ensure the integrity of the data, and ensure authorized users have timely, reliable access to data, while supporting accountability of all health professionals involved in accurately matching patients to their health information.
2. **Mitigate fraud by establishing minimum authentication capabilities within every system where a member, patient, employee, or vendor can access patient data.** Every system access point can present a vulnerability for potential fraud, and the strategy should be able to eliminate or substantially reduce identity theft or other fraud perpetrated against a patient.
3. **Encourage HIPAA covered entities to thoroughly document where and how electronic protected health information (ePHI) is being used, including by third parties.** Establishing patient trust will be bolstered by clear and transparent information concerning the uses of their health information.

Standardization

Approaches to patient identification and matching should be standards-based to align with ongoing national efforts around interoperability. The national strategy should:

1. **Define the minimum standardized data set needed for patient identification and matching.** The strategy should adopt a common set of specific demographic fields or data elements to be used for patient matching and a common set of standards for such data elements. The US Core for Data Interoperability could be one pathway to develop this minimum standardized data set.
2. **Encourage and facilitate ongoing collaboration with industry-based patient matching efforts, including those led by standards development organizations (SDOs) such as HL7.** Collaboration of this nature will increase buy-in and align with other federal efforts to improve standardization and interoperability.
3. **Encourage a standardized format for addresses, and potentially other data elements, to increase accurate patient matching rates**. Standardizing addresses has been found to be independently associated with improving matching accuracy.[26]

4. **Be compatible with existing principles and standards.** Compatibility with existing health data, identity, notice and consent, and interoperability standards will ensure consistent deployment across US healthcare organizations.
5. **Provide guidance on standardization of data capture and best practices processes post-mergers, during data conversions, and after closure of an institution.** Health systems are not static and must be prepared to maintain patient identification standards during periods of change. Guidance on standardized data capture and best practices will be necessary as health systems and clinician practices continue to consolidate.

Portability and Interoperability

As our national health system moves towards increased interoperability, so should discussions around patient identification. Addressing patient identification will reduce the burden on providers and the healthcare and public health systems as it ensures a more interoperable system. To ensure patient identity is portable and universally incorporated into an interoperable healthcare system, a national strategy around patient identification and matching should:

1. **Provide maximum achievable accuracy to avoid patient safety issues not only within systems, but across systems.** The ability to easily share patient information across health systems and insurance systems is necessary, and to protect patient safety, a national strategy should support doing so with the maximum achievable accuracy.
2. **Provide guidance on ensuring semantic integrity for information shared across systems.** The use of various systems should not preclude accurate and unambiguous health information transmission.

Data Quality

Data quality is one of the paramount considerations when interacting with health information and managing patient identity. To ensure adequate data quality, a national strategy around patient identification and matching should:

1. **Take a holistic approach and consider underlying and fundamental data integrity and quality processes and practices.** A national strategy must be complete, all-inclusive, and consider data integrity and quality across all stakeholders, including populations that have historically been disproportionately affected by patient misidentification.
2. **Provide the opportunity for patients to self-correct or flag aspects of their record.** Patients should be able to participate in the correction of inaccurate information in their own medical record.
3. **Be designed to minimize errors and fraud.** The strategy should be designed to minimize accidental errors and minimize options for intentional errors such as impersonations, identity theft, and data breaches.
4. **Provide guidance on the ability to recover quickly and inexpensively from errors.** The strategy should support the ability to correct errors in data that are used to establish identity and in downstream uses of data, including separating overlays, overlaps, and incorrectly merged records, in all locations where data is stored.
5. **Consider the timeliness of solutions.** A strategy should provide guidance around real-time identity management and timely resolution of errors.

Integration with current systems

The US healthcare system is currently served by a number of disparate systems, including systems for patient registration, clinical patient records, image data, patient generated health data, and consolidated longitudinal records within public health registries. Acknowledging these different systems, a national strategy around patient identification and matching should:

1. **Be able to integrate with as many current systems as possible, and as simply and inexpensively as possible, throughout the healthcare sphere.** The ease of ability for a strategy to be integrated into systems already in use will increase the uptake of the strategy by relevant healthcare organizations.
2. **Enable each of these integrated systems to achieve improved accuracy and performance.** Healthcare organizations have dedicated resources to help achieve accurate patient identification. A new strategy should enhance, not compete, with those efforts.
3. **Consider the time and resources needed for healthcare organizations to adopt the national strategy.** The strategy should consider the constraints healthcare organizations are under and work to support adoption of the strategy in the most efficient way possible.

Equity and Inclusion

Just as health is inherent in every person, being served by the healthcare system must also be inherent. To ensure every person within the US is served equally and equitably, the national strategy around patient identification and matching should:

1. **Be culturally sensitive and respectful and take into consideration the various ways different communities interact with and participate in the healthcare system.** Every community has had various histories of interactions with the medical systems in the US, resulting in differing levels of trust and participation. A national strategy must take these histories into account.
2. **Take into account disparate access to technologies and infrastructure in different communities and patient populations.** A national strategy must ensure the benefits of accurate patient identification are available to all people and promote equity.
3. **Be simple and easy to understand.** Simplicity will help bolster trust in the integrity of patient identification and matching.
4. **Be language independent.** Language independence will provide maximum clarity for those for whom English is not their native language.
5. **Support all potential patients.** Every patient has unique needs, and a national strategy must be able to support all potential patients, including children, those with nonpermanent addresses, and those with various naming traditions.
6. **Support caregivers.** A national strategy must take into account patients where identification is managed by a caregiver, who must be able to fulfill all the patient's identification and authentication requirements, and incorporate the ability to extend guardianship to the patient's identity and records.
7. **Be universally applicable and accessible.** A national strategy must take into consideration any person who needs medical care in the US, regardless of citizenship, insurance status, ability to pay, inadequate identification, and/or housing situation.

Sustainability and Governance

Sustained investments, governed appropriately, are needed to improve and maintain accurate patient identification and matching, which is necessary for a safe, high-quality, cost-effective, patient-centered US healthcare system. Patient identification and matching is a key priority and will help attain faster, more effective, and more efficient interoperability across healthcare and within public health ecosystems. To ensure sustainability and appropriate governance, the national strategy should:

1. **Have adequate funding for the creation and implementation of a national approach to address patient identification and matching, and for activities that support improved patient identification, including ongoing data and operability standards-related activities led by ONC.** Congress and the Administration must make funding for this initiative a priority to truly address patient identification and matching issues.
2. **Preclude cost-shifting onto patients.** The national

strategy for patient identity should preclude incurring any cost burden on patients and/or caregivers.

3. **Be designed to serve the US healthcare system for many years.** The strategy is an investment in the future of US healthcare; therefore it must be sustainable, have the capacity to support accurate patient identification for 100% of the US population for many generations, be future-proofed, nimble, flexible, and allow for an iterative process.
4. **Have governance that is public, transparent, and accountable.** Patient identification and matching is an issue that affects patients' safety and care all across the US, and therefore the governance of a strategy must inspire trust. Establishing a governance framework that is public, transparent and allows for stakeholder input will assist in building such trust.

Conclusion

Recognizing the importance of accurately matching patients to their health information must be a top priority in any interoperable healthcare system. The creation and implementation of a national strategy around patient identification and matching is possible through collaborative efforts between the private sector and federal government.

The successful formation of a national strategy around patient identification and matching will incorporate perspectives from across the healthcare ecosystem, including perspectives from physicians, patients, providers, public health, health IT, and other health information organizations. The Patient ID Now coalition is pleased to begin the work of coalescing these perspectives into a framework of considerations for the creation of a national strategy.

Appendix A: Work Group, Contributors, and Staff

Work Group Participants:

Meryl Bloomrosen, Senior Director, Federal Affairs, Premier healthcare alliance

Joe Cody, Associate Director, Research and Innovation Policy, American College of Cardiology

Victoria Dames, Senior Director, Product Management, Experian Health

David Gray, Director, Government Relations & Connected Health Policy, HIMSS

Barry Hieb, MD, Chief Scientist, Global Patient Identifiers, Inc.

Cherie Holmes-Henry, Vice President, Government & Industry Affairs, NextGen Healthcare

Mary Beth Kurilo, Senior Director of Health Informatics, American Immunization Registry Association

Tom Leary, Senior Vice President, Government Relations, HIMSS

Cassie Leonard, Director of Congressional Affairs, CHIME

Alana Lerer, Manager, Government Relations, HIMSS

Rob MacMillan, Chief Executive Officer, Global Patient Identifiers, Inc.

Aaron Miri, MBA, CHCIO, Chief Information Officer, Information Technology, Dell Medical School and UT Health Austin

Duanne Pearson, Vice President, Premier healthcare alliance

Karen Proffitt, MHIIM, RHIA, CHP, Vice President, Data Integrity Solutions, Just Associates

Lauren Riplinger, Vice President, Policy & Government Affairs, American Health Information Management Association

Mari Savickis, Vice President, Public Policy, CHIME

Karen Sealander, Partner, McDermott Will & Emery

Jim St. Clair, Chief Trust Officer, Lumedic, and Steering Committee Member, Trust Over IP Foundation

Amelia Suermann, Congressional Lobbyist, American College of Surgeons

Contributors

Leslie V. Albright, MBA/HCM, CHCIO, Member of CHIME

Bill Barnes, Federal Government Relations Director, Intermountain Healthcare

Katie Boyer, MPPA, Manager of Policy & Advocacy, Nemours Children's Health System

Jason Denson, Compliance and Ethics Director, Intermountain Healthcare

Donna Doneski, Director of Policy and Membership, National Association for the Support of Long Term Care (NASL)

Katie Gorris, Chief Privacy Officer and Compliance Director, Intermountain Healthcare

Stan Huff, MD, Chief Medical Informatics Officer, Intermountain Healthcare

Amanda Krzepicki, Manager, Government Relations, HIMSS

Julien Nagarajan, Manager, Government Affairs Mid-Atlantic & US Health Policy, RELX

Kasey Nicholoff, Program Manager, Electronic Health Record Association

Frank G. Opelka, MD, FACS, Medical Director, Quality and Health Policy, American College of Surgeons

Sid Thornton, Digital Impact Director, Intermountain Healthcare

Staff

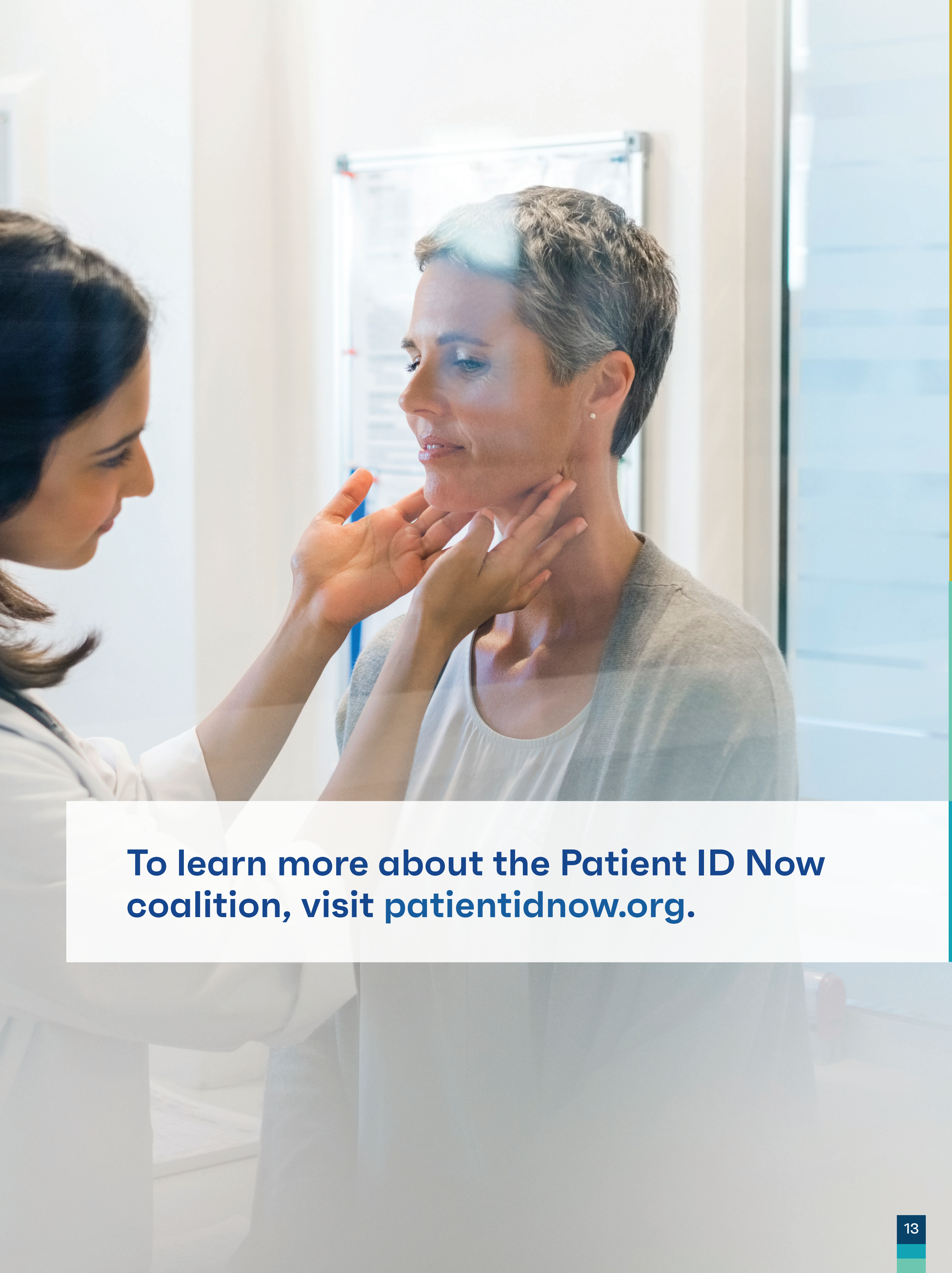
Kate McFadyen, Director, Government Affairs, American Health Information Management Association

Acknowledgement

We would like to thank all the member organizations of the Patient ID Now coalition for their work in the creation of this framework.

References

1. https://www.bmj.com/content/353/bmj.i2139
2. Top 10 Patient Safety Concerns for Healthcare Organizations, Available at: https://www.ecri.org/EmailResources/PSRQ/Top10/2017_PSTop10_ExecutiveBrief.pdf
3. https://www.prnewswire.com/news-releases/improving-provider-interoperability-congruently-increasing-patient-record-error-rates-black-book-survey-300626596.html
4. https://www.imprivata.com/patient-misidentification
5. https://standards.globalspec.com/std/1585864/ASTM%20E1714
6. https://www.rand.org/pubs/monographs/MG753.html
7. https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/pcast-health-it-report.pdf
8. https://bipartisanpolicy.org/report/challenges-and-strategies-accurately-matching-patients-their-health-data/
9. https://www.healthit.gov/sites/default/files/patient_identification_matching_final_report.pdf
10. https://www.congress.gov/114/plaws/publ255/PLAW-114publ255.pdf
11. https://www.rand.org/pubs/research_reports/RR2275.html
12. https://www.pewtrusts.org/en/research-and-analysis/reports/2018/10/02/enhanced-patient-matching-critical-to-achieving-full-promise-of-digital-health-records
13. https://www.healthit.gov/sites/default/files/safer/guides/safer_patient_identification.pdf
14. https://www.gao.gov/assets/700/696426.pdf
15. https://appropriations.house.gov/sites/democrats.appropriations.house.gov/files/HR%201865%20-%20Division%20A%20-%20LHHS%20SOM%20FY20.pdf
16. https://www.healthit.gov/news/events/2020-onc-annual-meeting
17. https://journal.ahima.org/a-realistic-approach-to-achieving-a-1-percent-duplicate-record-error-rate/?_ga=2.64359343.1442663878.1613576811-1355208103.1602095131
18. https://www.healthit.gov/buzz-blog/health-it/say-hey-to-project-us-a-unified-specification-for-address-in-health-care
19. Harris, Shannon and Shannon H. Houser. “Double Trouble—Using Health Informatics to Tackle Duplicate Medical Record Issues.” *Journal of AHIMA* 89, no. 8 (September 2018): 20–23. http://library.ahima.org/doc?oid=302567.
20. Landsbach, Grant. “Study Analyzes Causes and Consequences of Patient Overlay Errors.” *Journal of AHIMA* 87, no.9 (September 2016): 40-43. https://bok.ahima.org/doc?oid=301860.
21. AHIMA Work Group. “Managing the Integrity of Patient Identity in Health Information Exchange (2014 update).” *Journal of AHIMA* 85, no.5 (May 2014): expanded web version. https://library.ahima.org/PB/PatientIdentityHIE.
22. https://ahima.org/media/m1pldevh/ahima-pim-whitepaper.pdf
23. http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html
24. https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf
25. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/minimum-necessary-requirement/index.html#:~:text=The%20minimum%20necessary%20standard%20requires,disclosure%20of%20protected%20health%20information.
26. https://academic.oup.com/jamia/article-abstract/26/5/447/5372371?redirectedFrom=fulltext



To learn more about the Patient ID Now coalition, visit patientidnow.org.

PATIENT ID NOW

Framework for a National Strategy on Patient Identity

134.21