A report from THE PEW CHARITABLE TRUSTS | Oct 2018

Enhanced Patient Matching Is Critical to Achieving Full Promise of Digital Health Records

Accurately linking individuals with their records essential to improving care

Contents

The Pew Charitable Trusts

Susan K. Urahn, *executive vice president and chief program officer*
Allan Coukell, *senior director*
Josh Rising, *director*
Ben Moscovitch, *project director*
Rita Torkzadeh, *officer*

External reviewers

Pew's health information technology project wishes to thank the following for their comments on the draft report: Jitin Asnaani, CommonWell Health Alliance; Hans Buitendijk, Cerner; Matt Doyle, Epic; Keith Hanna, IPRD Group; Aaron Miri, formerly with Imprivata; Michelle De Mooy, formerly with the Center for Democracy & Technology; Shaun Grannis, Regenstrief Institute; John Halamka, Beth Israel Deaconess Medical Center; Elizabeth Harrington, Public Opinion Strategies; Beth Haenke Just, Just Associates; Ryan Howells, Leavitt Partners and CARIN Alliance; Grace Koh and Mark LaRow, Verato; Keith Fraidenburg, College of Healthcare Information Management Executives; Robert S. Rudin, RAND Corporation; Catherine Schulten, LifeMed ID; Jeffery Smith, American Medical Informatics Association; Joe Trelin, CLEAR; and Micky Tripathi, Massachusetts eHealth Collaborative. Although they have reviewed the report, neither they nor their organizations necessarily endorse its findings or conclusions.

Acknowledgments

We further thank current and former Pew colleagues: Emily Banks, Zach Bernstein, Laurie Boeder, Gaby Bonilla, Kimberly Burge, Tim Cordova, Casey Ehrlich, Mary Markley, Erin McNally, and Bernard Ohanian for their valuable editing and production assistance on this report.

Cover photo:
Ann Cutting

Contact: Laurie Boeder, communications director
Email: lboeder@pewtrusts.org
Project website: pewtrusts.org

Overview

The way patients receive medical care has drastically changed over the past decade as most hospitals and doctors' offices have transitioned from paper charts to electronic health records (EHRs) that help clinicians order medications, document treatment decisions, and review laboratory results. These digital records can introduce numerous efficiencies and give patients and medical professionals more complete information on which to base decisions.

Yet in order for patients, doctors, nurses, and other clinicians to have this information, EHRs must be able to share data among the many different hospitals, offices, and other facilities where individuals seek care—especially when health care providers are seeing new patients and need to obtain information from previous care providers. Effective data exchange also helps clinicians get information to treat individuals with chronic conditions—approximately a third of Americans—and older adults, who often see more than 10 different physicians at dozens of office visits per year.

The successful exchange of health information—known as interoperability—depends on several factors, including a desire by institutions to share data; the use of effective standards and interfaces for depicting and communicating the information; the protection of patients' data; and the capacity to successfully search each individual's record in disparate locations and know that it refers to the correct person.

This report focuses on the last problem—patient matching—while also recognizing that many other challenges remain for effective and robust interoperability.

Patient matching helps address interoperability by determining whether records—both those held within a single facility and those in different health care organizations—correctly refer to a specific individual. Unfortunately, patient matching rates vary widely, with health care facilities failing to link records for the same patient as often as half the time. Deficiencies in matching patients to their records can lead to safety problems: For example, if an allergy listed in one record is not documented in another, or if records for two different individuals are incorrectly merged, patient harm can occur. In a 2012 survey conducted by the College of Healthcare Information Management Executives (CHIME), 1 in 5 hospital chief information officers indicated that patients had been harmed in the previous year due to mismatches.

Failures to effectively match patients can also be costly, leading to repeat tests and delays in care. In an extreme example, the care for an 11-month-old twin was documented in her sister's record, resulting in the failure of the health system to recoup $43,000 in costs from the insurer.

Inadequate patient matching has generated interest among federal policymakers. The 21st Century Cures Act—signed into law in 2016—requires the Government Accountability Office to examine steps taken by the federal government and the private sector to reduce matching errors. In the same law, Congress also required the Office of the National Coordinator for Health Information Technology (ONC, the federal agency that oversees EHRs) to develop a policy to support the exchange of information on a nationwide scale. In implementing the policy, known as the Trusted Exchange Framework and Common Agreement (TEFCA), ONC has proposed creating a series of health information networks and an independent organization to govern them. Success of the effort relies on adequate patient matching.

To address patient matching challenges, The Pew Charitable Trusts conducted research to assess various opportunities to make progress. Following conversations with matching experts and an examination of public reports and documents, Pew evaluated a number of common suggestions, emerging approaches, and other

strategies that the private sector and government can take to improve patient matching, including the creation of a unique identifier for patients; the establishment of patient-empowered solutions, enabling each individual to ensure that his or her records are matched; standardization of demographic data, such as addresses; and the use of more information sources to verify a person's identity, known as referential matching. Pew commissioned studies of key topics, interviewed hospital and clinician executives, held focus groups with patients, heard from experts, and examined the existing literature.

The research revealed common themes. First, regardless of the approach taken, a nationwide strategy will require coordination to identify the needed best practices; commitments from health care organizations and technology developers to implement agreed-upon standards; and patient involvement. Second, no solution currently exists that could achieve perfect—or even near-perfect—match rates for all patients, but actions can be taken to better link records. Third, although some opportunities exist to make meaningful, incremental progress in the near term, more robust change will require the use of new approaches and technologies.

This report lays out Pew's research findings and recommendations, including steps that can be taken in the near term to improve matching and the infrastructure needed for more robust progress in the medium term and long term.

Near-term activities to help make incremental progress include the following: clarification of restrictions on government funding for unique identifiers; agreement on demographic standards; assessment of privacy ramifications; further research on and adoption of referential matching, where third-party data are used; and verification of phone numbers and other identifying information provided by patients to reduce the likelihood of typographical, data-entry, or clerical errors.

Long-term opportunities to develop the infrastructure include the following: entrusting a single organization to oversee a nationwide patient-matching strategy; launching pilot projects for patients to use their smartphones to help match records; and determining the infrastructure and standards necessary for using biometrics and other technologies for effective and secure matching in a way that protects privacy.

Once these recommendations are implemented, clinicians and patients can have more assurance that EHRs contain complete, accurate, and up-to-date medical information—thus improving safety, reducing costs, and better coordinating care for individuals who see multiple medical professionals.

Current match rates and challenges to progress

The rate at which patients are accurately matched to their records varies widely across institutions and differs based on whether the matching occurs within a facility's own systems or between organizations. Several factors affect match rates, including the technologies and processes employed and the quality of data collected.

Match rates vary widely

According to one estimate from CHIME, matching within facilities can be as low as 80 percent—meaning that 1 out of every 5 patients may not be matched to all his or her records when seeking care at a location where the patient has been seen.[1] Organizations can, though, achieve match rates of 90 percent or higher when the organization maintains high data quality and manually checks and fixes uncertain matches.[2]

Match rates between organizations can be far lower. Audacious Inquiry, a contractor that has conducted research for ONC, found match rates as low as 50 percent even between organizations that share the same EHR vendor because of the variability in technology and processes.[3] On the other end of the spectrum, though, one company claims that its technology can match records for adult patients with 98 percent accuracy.[4]

Intermountain Healthcare took wide-ranging measures to increase its match rates from 10 percent to 95 percent when exchanging data with the University of Utah. Intermountain implemented data validation checks, data normalization, and data-cleansing steps to address data quality issues and achieved match rates above 60 percent. Additional technical and operational actions, including optimizing matching attributes and algorithm functions, were done in cooperation with the University of Utah to push match rates to 95 percent.[5]

However, organizations generally face challenges in accurately calculating match rates because they lack definitive information on which records should be linked. The inability to know all the correct matches directly reflects matching challenges; instead, health care facilities know only how many records they have successfully matched.

Both false positives (meaning records are incorrectly merged) and false negatives (which refers to the frequency that patients have unlinked records or when facilities cannot locate patients' existing records within other organizations, resulting in the creation of duplicate records) can lead to adverse events.[6] One report from 2016 indicates that 4 percent of confirmed duplicate records results in negative clinical care, such as delays, lack of access to diagnostic results, and duplicated tests.[7] For example, false negatives can contribute to clinicians not seeing key test results or allergy lists, which could lead to individuals getting treatment that should be avoided. False positives could result in patients getting treated based on someone else's information, including incorrect diagnoses or unneeded medications.[8]

Given that matching rates are calculated differently across health care facilities, making comparisons between institutions is challenging. On the whole, health care institutions err on preventing false positives; consequently, failure to link patients to their own records is the more common problem.

ONC, as part of its interoperability roadmap published in 2015, set goals for duplicate records within a health care facility.[9] ONC sought to have less than 2 percent duplicate records within facilities by the end of 2017, and 0.01 percent by 2024. Few data exist, on a national scale, to indicate progress toward that goal, though recent analyses indicate that the industry has fallen short of ONC's goals. A 2018 survey from Black Book Market Research revealed that an average of 18 percent of patient records within organizations are duplicates, which is consistent with what some technology vendors have reported.[10] ONC did not set a goal for accurately matching records between facilities.

The Importance of Improved Match Rates

Patient matching is an essential prerequisite—and is currently one of the barriers—to enhanced interoperability.[11] Once higher patient matching rates exist and the other challenges to interoperability are addressed, enhanced sharing of data can:

- *Improve patient care and satisfaction:* Patients and clinicians rely on having access to the most up-to-date information on laboratory results, the individual's current medication regimen, family medical history, and myriad other data points that can change the care provided. Enhanced patient matching can ensure that clinicians and patients have this information, helping individuals receive safer, higher-quality care by mitigating the likelihood of clinicians using incorrect or incomplete information.
- *Reduce costs:* Improved patient matching rates can also reduce health care costs in several ways. First, health care providers currently spend significant resources, including staff time, to merge duplicate records for the same individual and fix records that are incorrectly combined.[12] Children's Medical Center Dallas found that having duplicate records cost $96 per record on average.[13] Separately, the Mayo Clinic has spent hundreds of thousands of dollars to resolve some of these errors.[14] Second, inadequate patient matching can lead to duplicate tests and other procedures when clinicians must reorder them because the findings are stored in health records located elsewhere.[15] The Black Book survey found that repeated services because of duplicate records cost on average $1,950 for each patient per hospital stay.[16] Black Book also found that hospitals can lose revenue when health insurance claims aren't paid, finding that a third of denied claims stem from patient identification inaccuracies. This cost hospitals $1.5 million on average in 2017.
- *Support innovation:* Improved matching can also help researchers better track patient outcomes over time and when individuals seek care from multiple locations. For example, researchers studying a drug could get better data on patient outcomes over several years and from different hospitals and specialists seen by a patient. As a result, enhanced matching can support better clinical trials and the use of real-world evidence to study health care quality and costs.
- *Detect fraud:* In some cases, patients' information may be stolen and used.[17] For example, an individual may seek care using the information of a different person to avoid paying for services. The individual whose information was illicitly used could then face bills for the care or have his or her insurance cover the costs. Better patient matching, in some cases, may be able to help detect and prevent this type of fraud.[18]

Contributing factors to inadequate match rates

Patient matching challenges arise from different causes, including the following:

- *Standardization:* Each data element may not be standardized in the same way across health information technology (IT) systems. For example, one system may list addresses in a single field, while another may separate street names from the city and state.[19]
- *Typos:* Information can also be entered incorrectly, such as the transposition of numbers in a birthdate or the inaccurate spelling of a last name.
- *Information not entered:* Data may also not be entered in the first place. For example, not every patient may provide an email address, or the health care system may fail to ask for and document it out of concerns that it would slow down registration. Similarly, some EHR systems may include only patients' middle initial, not the full middle name.
- *Default or null values:* Key identifying fields may have preset values to indicate unknown or missing information.[20]
- *Similar information:* Patients also may have similar information. For example, twins can share the same birthdate and address, and can have similar names. And, in some regions, certain names are extremely common. A health system in Houston found 2,488 records with the name Maria Garcia, of which 231 shared the same birthdate; many of these probably refer to the same individual.[21]
- *Information changes:* Patients move, get married, and undergo many other life events that can affect the demographic information in their records. When this occurs, the data may not match between systems.
- *Identity fraud:* Patients may use someone else's information to get treatment, which introduces erroneous data in a person's health record. A 2016 study of 555 errors over a five-year period in one health care organization found that approximately 2.5 percent of false positive matching errors resulted from fraudulent activity as opposed to other factors.[22]
- *Ineffective for some populations:* Some patient populations—particularly children or individuals with lower socioeconomic statuses who don't have certain identifiers or who often move—may have unknown or nonstatic demographic information. Similarly, some patient populations—such as undocumented immigrants—may be reluctant to provide accurate information out of fear of deportation. As a result, the use of demographic data elements for matching may be less effective in these populations.

How matching is done today

Patient matching—whether within an individual organization or between facilities—typically occurs through the use of algorithms, unique identifiers, manual review, or a combination of these methods, with a survey of health care chief information officers published in 2012 finding that 42 percent of respondents rely on two or more strategies.[23]

Algorithms serve as foundation to matching

Mathematical algorithms use demographic data derived from electronic health records as the foundation to the matching processes. Given the pervasive use of algorithms for matching, the inadequate match rates achieved within and between organizations typically refer to the use of this approach, though different algorithms have varying capabilities that affect their performance.

Commonly used demographic data elements include patients' first and last names, date of birth, Social Security number, and address. Less common data elements can include cellphone numbers or email addresses; this information does not necessarily change when patients move.[24] For example, a Pew Research Center study found that 10 percent of adults have an out-of-state cellphone number.[25] Additionally, some technology vendors indicated that algorithms may also be able to use previous addresses and names, which are not typically incorporated into matching approaches today.

Algorithms have classically fallen into three broad categories, although each organization may use multiple approaches.[26]

- *Deterministic:* With deterministic algorithms, several data elements must match exactly—without any typos or variation.
- *Rules-based:* Under rules-based algorithms, each data element receives a "weight" for how essential it is to match a record. Even if not every data element matches exactly, the records will match so long as enough data elements are identical. In essence, these algorithms include various rules that allow for different permutations of the data elements. If the data elements within one of those permutations are the same, then the records will be matching (for example, records will be matched if first name, last name, date of birth, and gender match or records will be matching if last name, address, and date of birth match).
- *Probabilistic:* Among the more sophisticated matching techniques, probabilistic algorithms provide health care organizations with the likelihood that two records refer to the same individual even if typos or other irregularities exist in the data. These algorithms often factor in, for example, that letters can be transposed or that a patient moved addresses when, on the whole, the data suggest it is the same person. Individual health systems can fine-tune their algorithm based on the unique aspects of their patient populations (for instance, if a given first or last name is prevalent in the geographic area near a hospital, the facility can weight that name less than institutions in regions where that name is uncommon).

Some common algorithm-based approaches include the following:

- *Built into EHRs:* Both EHR vendors and other health information technology companies have developed their own matching systems based on the types of algorithms listed above. For example, users of an EHR system can leverage the matching algorithm included in that product or choose to use the matching software provided by third-party vendors.

- *The Sequoia Project:* Sequoia, a nonprofit organization that advances nationwide interoperability, administers the interoperability frameworks called Carequality and eHealth Exchange.[27] These systems enable different health care facilities to exchange information on a patient. Each participating facility uses its own matching software to indicate whether it has a match for a patient. Sequoia is in the process of developing a minimal set of practices relying only on existing technologies for cross-organizational patient matching for its members. The organization has issued a report with best practices to increase organizations' matching rates.[28]
- *CommonWell Health Alliance:* CommonWell Health Alliance, a not-for-profit association of technology companies, also operates a network for the exchange of health information and uses a custom algorithm to conduct matching. When common identifiers are available—such as state- or health-system-wide ones—these are used by the algorithm to improve match rates. End users, such as front-desk staff at health care facilities, can also ask patients to verify encounters with other providers to support more accurate matches.[29]

In June 2017, ONC held a competition to compare the effectiveness of different algorithms on a database of identities provided by the agency to spur interest in measuring the performance of different algorithms.[30] The competition compared algorithms on false positive and negative rates, among other criteria.[31] But the findings may not reflect the real-world ways in which matching challenges can arise because of the use of synthetic data, which is created and corrupted using computers. The three winners of the challenge employed different algorithms, and all required some amount of manual review to adjudicate complicated linkages. The Agency for Healthcare Research and Quality is also funding research to study the effects of different algorithm enhancements.[32]

Other key aspects to current matching approaches

In addition to algorithms, several other factors influence the ability of organizations to match records.

Health care organizations often maintain master patient indexes—databases that contain demographic information for a facility's patients—to keep an up-to-date roster of the individuals for whom they have records. Patients listed in these indexes often have one or more site-specific unique identifiers associated with them, but those are often not shared externally.

Data quality—such as the prevalence of typos—can also affect match rates; some organizations have emphasized addressing this challenge. In December 2017, ONC released a series of best practices to help ensure better data quality, such as for organizations to establish quality assurance programs.[33] Similarly, the ECRI Institute has also developed recommendations, including on data validation.[34]

Additionally, some organizations have employed the use of third-party data derived from non-health care sources—such as credit bureaus—to aid with matching.[35] This approach, referred to as referential matching and described in more depth later in this report, can help make matches even when patient demographic data changes.

Finally, organizations often tune their algorithms to reflect their unique patient populations. For example, organizations that treat high Latino populations may adjust their algorithms to de-emphasize the weight of names more common to those individuals. Alternatively, some cultures have a high proportion of individuals who share the same birthday—such as Jan. 1—for various reasons, and health care organizations may adjust their algorithm to accommodate those population-specific nuances.[36]

Despite progress and the use of innovative approaches, match rates remain insufficient to comprehensively and accurately link records on a nationwide scale.

Table 1

Typical Life Cycle of a Match

	1 Data collection	2 Data validation	3 Identity matching process	4 Clinical or administrative action
	Capture of key demographic data needed to verify identity and support matching process	Validation of data required to support organization matching process Application of matching algorithms to available data	Determination of whether a match has been obtained Combination of automated (electronic) and manual processes depending on organization policies and sophistication of electronic tools and processes	Based on output of matching process, execution of treatment, diagnostics, or medical records action (e.g. create new record or append information to an existing record)
Intraorganization				
Patient presents in person	Registration and identity verification, usually of data obtained from patient during registration process	Match based on registration data	Automated and manual processes	New record created *-OR-* Existing record updated
Interorganization				
Solicited inbound record from external system (e.g. hospital requests record from specialist)	Electronic data processed from record or record request	Match based on data provided by record sender	Automated and manual processes	Existing record updated
Unsolicited inbound record from external system (e.g. specialist sends primary care physician assessment)	Electronic data processed from external source is received	Match based on data provided by record sender	Automated processes	Existing record updated *-OR-* Orphan record, probably discarded
Unsolicited request for record from external system (e.g. hospital requests record from primary care physician)	Electronic data processed from record request	Match based on data provided by requester of record	Automated processes	No record returned *-OR-* Record returned

Topics examined by Pew and research approach

Pew examined four main approaches to improve patient matching, each selected based on common recommendations and discussions with experts. These approaches, described in more depth later in this report, include the following:

- *Unique identifiers:* Development of a unique identifier system that unambiguously identifies an individual and can link that person to his or her records associated with that identifier. This approach could include a unique number, use of a smart card with an encoded number, or biometrics.
- *Patient-empowered approaches:* Establishment of a process for patients to ensure their records are matched completely and correctly. Under this approach, patients would bear some ability to help health care facilities match their records.
- *Demographic standards:* Refinement of demographic data standards. Many experts have recommended that organizations use the same demographic data elements—formatted in the same way—to improve matching. Pew tested whether standardizing each data element yields benefits.
- *Referential matching:* Use of data collected outside of health care. Data from credit bureaus and other organizations contain demographic data for individuals. This information can be used to help match individuals' records, including when information changes.

In addition, Pew—in conjunction with John Halamka, chief information officer of Beth Israel Deaconess Medical Center—convened approximately two dozen experts on patient matching in July 2017 to identify the key characteristics needed for a successful nationwide strategy. The expert group concluded, among other recommendations, that a single organization should have the responsibility to oversee and advise on ways to improve patient matching and incorporate new technologies and approaches as they emerge. This organization would identify and encourage adoption of certain standards—such as on biometrics or use of smartphones—by health care organizations and technology developers.

To evaluate each of these topics, Pew spoke with experts from technology companies, hospitals, government, and other organizations, and examined published literature. In some cases, Pew also commissioned independent research and sought input from patients and health care executives.

Patient focus groups conducted

Pew held focus groups with patients to understand their perspectives on the aforementioned approaches to matching. Pew worked with Public Opinion Strategies (POS) and Hart Research Associates to conduct 11 focus groups with a total of 95 participants in five cities: Richmond, Virginia; Denver; Nashville, Tennessee; Houston; and Philadelphia.

Each of the focus groups elicited the feedback of a distinct patient population: Democrat primary voters; Republican primary voters; frequent recipients of health care services; infrequent recipients of health care services; parents of young children; family caregivers of individuals with serious illness; and Medicare beneficiaries. Two focus groups were conducted with each of the first four populations listed. POS and Hart developed screening tools to identify participants from each of the populations, as well as an interview guide to help uniformly administer the focus groups.

On the whole, participants expressed support for enhanced interoperability—fueled by better matching—to give patients and clinicians more timely access to data, though they expressed concerns about the prospects of information being stolen, privacy, and the sale of the data. Although patients were segmented into different subpopulations, they expressed consistent attitudes and reactions to patient matching and the options discussed across the groups. The modest differences—such as more skeptical views of government involvement by Republican primary voters—were greatly outweighed by the overall consistency in responses.

Health care executives interviewed on matching

Pew also collaborated with the Massachusetts eHealth Collaborative (MAeHC)—a nonprofit organization that convenes experts from technology developers, health care providers, and other groups—to interview executives at hospitals and doctors' offices on patient matching.

MAeHC developed an interview guide to obtain information on current match rates, challenges faced by organizations, factors that would influence additional investments to enhance matching, and various approaches to make progress. The interviews occurred with two dozen leaders from U.S. health care organizations representing large and small hospitals, critical access facilities, academic medical centers, ambulatory care clinics, and organizations that support interoperability between these facilities. Some organizations have national reach, while others serve only local populations. The individuals—many of whom were senior executives—all had responsibility for patient matching and interoperability, and had sufficient authority to guide investment decisions. Several key, overarching findings emerged from these interviews.

Interorganization offers biggest opportunity for progress

Health care providers interviewed have focused to date on matching within their facilities; however, demand for interorganization matching is increasing for several reasons. First, health systems are consolidating and require additional tools to match within affiliated—but separate—facilities. Second, the focus on alternative payment models and accountable care organizations that encourage care coordination increases the demand for better matching. And automation to retrieve records held in different locations—including laboratories and pharmacy information systems—requires better matching techniques.

Match rate goal tops 99 percent

Interviewees unanimously indicated a desire to have match rates above 99 percent, though they lacked a consistent way to measure progress to that goal. Nearly every interviewee faced challenges articulating a current match rate, and frequently they included caveats that they could determine only their internal rates. Some organizations calculated only the number of duplicate records that they were able to identify, which falls short of detecting an internal match, let alone with external partners. Duplicate-record-creation rates measured ranged from 0.77 to 6 percent.

Investments being made

Many interviewees indicated that they have already invested in software to enhance matching and had dedicated staff—ranging from 0.5 to nine full-time employees—to manage record linkages. Both the software and personnel investments lead to the perception of patient matching as expensive to resolve.

Diminishing returns

As patient matching rates improve, interviewees indicated greatly diminishing returns on investments and the ability to make incremental improvements using existing technologies. For example, increasing match rates from 50 to 55 percent may be much simpler and less costly than advancing from 90 to 95 percent.

Organizations with lower match rates may find less expensive opportunities to significantly improve match rates, such as through enhancing the quality of data captured at registration or better tuning their matching algorithms to reflect unique attributes of their patient populations.

On the other hand, facilities with higher match rates find few opportunities to make improvements absent a paradigm shift in the processes or technologies they use. For these—which would therefore require substantially greater investments to make incremental gains—resource demands would collide with other institutional priorities that may have greater near-term quality, safety, or efficiency benefits.

Opportunity 1: Unique patient identifiers

Policymakers, experts, and individuals across the entire health care ecosystem often suggest a seemingly simple solution to patient matching: the use of unique patient identifiers or similar identifiers that have a high likelihood of referring to a given person. These identifiers—such as a number or biometric (facial recognition, for example)—would be used by patients to identify themselves at the point of care and would be associated with each record. The identifier would serve as a common, ubiquitous way to link that person's records and could be used in conjunction with other information, such as demographics, to enhance their utility.

In the United States, Social Security numbers (SSNs) have often been used as a unique identifier for health care, but this approach has limitations and—even when SSNs have been used—has not solved the matching problem completely. Several challenges exist:

- SSNs can be entered incorrectly into a record, which would hinder the ability of algorithms to rely solely on this data element for matching. One challenge to the use of SSNs is that they lack "check digits," which are part of an identifier that provide the opportunity to detect typos through, for example, ensuring that two digits add up to a certain value.
- The threat of identity theft may increase the reluctance of individuals to provide this sensitive information and providers to collect it.
- Occasionally individuals use someone else's SSN—either as part of fraud or because it is the identifier used for their health insurer, such as Medicare.
- There may be restrictions to the use of SSNs for purposes other than Social Security. For example, the Social Security Administration authorizes the use of SSNs for certain purposes; health care is not on the authorized list.[37] Some states have enacted laws restricting the use of SSNs, including for health care purposes.[38]
- The use of these numbers in health care is waning; the Centers for Medicare & Medicaid Services (CMS)—in response to federal legislation—is removing SSNs from Medicare cards and using a new numbering system instead. Those new numbers apply only to a portion of the population—Medicare beneficiaries—and do not link to records for individuals prior to their enrollment in the federal health insurance program. Potential expanded use of Medicare numbers is discussed below.

U.S. law prohibits the Department of Health and Human Services (HHS) to use its funds to create a unique patient identifier absent explicit new approval from Congress. Although the Health Insurance Portability and Accountability Act of 1996 requires HHS to develop a unique identifier, subsequent federal appropriations language has prohibited its implementation. In recent years, congressional appropriators have signaled that, although the prohibition stands, the federal government may provide guidance to the private sector in its efforts. Regardless, the federal appropriations language impedes progress on a national health identifier until Congress lifts the funding prohibition.

Meanwhile, many health care systems outside the United States use this approach for matching by leveraging national identifiers. For example, both Israel and China have citizens use their national ID as their patient identification number.[39] Similarly, New Zealand offers a National Health Index number to every individual who uses the country's health and disability services.[40]

Deficiencies persist for a government-led identifier

However, government-issued national numeric identifiers still face challenges and have not fully resolved the matching problem. For example, individuals in the National Health Service in England may choose not to use their ID numbers or the ID may not be checked by hospital staff, which can lead to misidentification and creation of multiple records.[41] According to one National Health Service analysis, 4.8 percent of patient safety reports associated with identification were related to failures in matching the unique agency identifier. In one case, blood samples were processed for the wrong patient because of a similar name; in another case, the unique identifier was not used, resulting in twins being mixed up.[42] In other cases, the incorrect National Health Service number was used.

Even in the United States, there are analogues to a unique identifier that have proven insufficient. For example, members of the armed forces and veterans have military identifiers, yet matching problems persist—especially with the private sector when those identifiers are not recorded.[43]

The creation of a government-issued numeric health identifier for all patients may also be expensive. The transition from SSNs to the new Medicare identifier could cost hundreds of millions of dollars. CMS estimated in 2011 that it could cost more than $800 million, and Congress provided $320 million for the effort in the Medicare Access and CHIP Reauthorization Act.[44]

Alternatively, some states have attempted to create their own health identifiers.[45] A 2009 Nevada law requires the examining of a unique patient identifier, and legislation passed in Minnesota in the mid-1990s further allows the state government to create such a system.[46] Since passage of those laws—one more than two decades ago—progress has not been made at the state level and is likely to face the same challenges as a federal identifier. Further, many patients seek care across state lines; state-based identifiers may not support matching for those individuals unless all states coordinate to identify the same—or at least compatible—approaches.

Finally, the use of alphanumeric identifiers in health care may represent technology that will probably become obsolete. These identifiers must be carried with patients and are susceptible to key-entry errors or patients forgetting them. Instead, emerging technologies—including biometrics and use of smartphones—may be able to serve as unique identifiers or otherwise authenticate the identity of an individual in a manner that could be used for matching.

Examples of Possible and Attempted Unique Identification

In lieu of a federal identifier, the private sector has examined ways it can advance a unique identification system and leverage the government's current programs.

- *CHIME:* To encourage the development of an innovative solution, the College of Healthcare Information Management Executives (CHIME) in 2016 launched a competition to award a $1 million prize to the individual or organization that can identify patients with 100 percent accuracy while protecting privacy.[47] Although CHIME selected four finalists, the organization

Continued on next page

suspended the competition in late 2017 after concluding that the goals were not met.[48] Although information is scant on the details of each finalist's proposal, public information released indicates that several solutions involved biometrics.

- *Authenticators:* Some hospitals employ technology in which patients use authenticators to assert their identity. Authenticators are something the patient knows, has, or is, which can include a biometric, a text message to the patient's smartphone that requires a response from the patient, or a personal identification number, among many other options. When such a system is implemented, facilities may require that two or more authenticators accurately match what the organization has on file to verify the patient's identity in multiple ways, known as multifactor authentication.
- *Social Security Number removal initiative:* The replacement of SSNs with a new Medicare identifier could provide an opportunity for private health plans to use the same system for identification. In 2015, Congress required CMS to remove SSNs from Medicare cards.[49] In implementing this provision, CMS intends by April 2019 to replace SSNs with an 11-character identifier composed of numbers and uppercase letters. Theoretically, CMS could allow private insurers to also use this system. If that were to occur, this number could remain with patients when switching insurers and serve as a de facto unique identifier. Doing this would require significant changes. For example, it could require CMS either to assign the unique numbers or turn over the issuing of identifiers to a private sector organization.

Biometrics offer opportunities

The use of biometrics—the measurement of physical characteristics that can help identify individuals—reflects an emerging trend. Airports, amusement parks, and sports venues are increasingly adopting biometrics at entrances, and people regularly use their smartphones to scan faces and thumbprints to unlock the devices. Hundreds of hospitals across the country have implemented some type of biometric—including palm vein and iris scans—to identify patients. One hospital found that more than 90 percent of patients agreed to use a biometric system for identification. These examples, though, focus on locating an individual's records within the implementing facility, not matching data across multiple institutions.[50]

Proponents of biometrics contend that they are highly useful for identification. Biometrics typically do not change for an individual, cannot be forgotten (unlike a password or card), and—especially when combined with demographic data—can be virtually unique to every individual.

Organizations can use different types of biometrics. This introduces challenges to matching among organizations that don't use the same modality, which refers to the biometric captured, such as fingerprint scans or facial recognition. For example, a health care facility that uses palm vein scans to identify patients may not be able to match patients with a facility that uses iris scans. Even within modalities, variability in how the information is captured and depicted electronically across different vendors hinders their utility for matching across institutions.

Security and privacy critical

The ubiquity and stability of biometrics—which contribute to their effectiveness for identification—increase scrutiny to ensure that they can be used in secure ways and that patient privacy can be protected. Biometrics—unlike passwords, for example—can't be changed. Once an individual's unprotected biometric data are obtained by criminals or unapproved individuals, then the data are compromised without the individual being able to change them. Further, some biometrics can be accessed publicly—such as facial recognition in a public place—and some can be spoofed. Researchers have created 3D print molds of fingerprints using a stored image, which can then be used in nefarious ways.[51]

Given the privacy risks associated with biometric use, technology developers, government, and other organizations are striving to address these challenges. Developers incorporated liveness checking mechanisms in technologies to detect, for example, whether the fingerprint originates from an artificial mold or if patterned contact lenses occlude an iris image.[52] Vendors have also encrypted data and incorporated other security tools to help mitigate privacy concerns. In parallel, privacy advocates and some state lawmakers are proposing bills to address concerns about the collection and use of biometric data, for instance to ensure the consent of individuals.[53] Regardless, the transmission of biometric data among organizations represents a potential privacy risk that must be mitigated for this approach to have viability in the marketplace.

Use of different modalities

The use of biometrics requires that they be scanned and converted into data that can be matched against a database. Different biometric modalities have their own benefits and drawbacks. Biometrics are highly precise, though the level of precision can vary based on the modality used, and the costs to deploy differ. Iris scans,[54] for example, can be among the most accurate, while fingerprint technology can be deployed at low cost.[55] The National Institute of Standards and Technology has evaluated different biometric modalities, focusing on face, fingerprint, and iris recognition.[56]

At the same time, facial recognition is accelerating in prevalence as smartphones incorporate this technology. The penetration of biometrics in the smartphone market also offers the opportunity for biometrics to be scanned on technology at a facility or on a patient's own device. Biometrics can be used as an authenticator in conjunction with other information to validate an individual's identity.

The Bill & Melinda Gates Foundation is piloting the feasibility of using biometrics in South Africa as an option for uniquely identifying patients and matching records across organizations. It seeks to introduce low-cost iris scanning into health care facilities and store the identifying information and scans virtually. As patients visit other health care providers or clinics, the biometrics scanned at each facility can be compared with those stored in the virtual database. The project aims to improve the linkage of laboratory records by tracking and retrieving everyone's information regardless of the clinic that patients visit.

Technology underpinnings of biometric use

Regardless of the modality used, biometric vendors follow similar processes for scanning and using the data. Vendors convert biometric scans into templates, which are a set of selected features or characteristics of the modality that correlate to an individual with a high degree of certainty and uniqueness. As templates typically vary across biometric vendors, it is often not possible to compare templates derived in different ways.[57] One example of an interoperable template is for fingerprints, for which there is a standard, and efforts underway to use it across different vendors via the Minutiae Interoperability Exchange, a program of the National Institute of Standards and Technology.[58]

Biometric vendors can further secure data by hashing the information. Hashing is a technique to render data indecipherable absent the use of a special translation tool—known as a key—to understand the data. For unauthorized users of individuals' biometrics to use the data, they would need to know how to decipher both the template and the hash.[59]

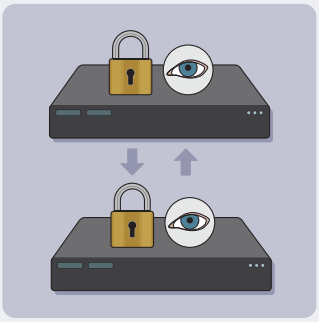
Biometric vendors use software called matching engines to compare data derived from an individual with the information contained in their identity database. This matching engine translates the template in a manner that can be used to link a record with an individual.[60]

Potential Biometric Models

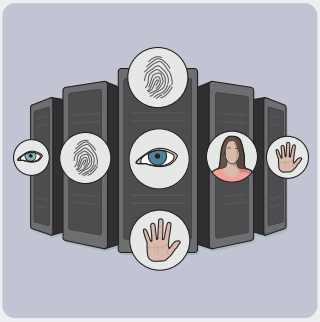
Several options could work for creating an infrastructure to use a single or multiple biometric modalities for matching, though the use of multiple modalities is probably preferable to accommodate different user needs, such as when someone with missing fingers can use a face scan. Additionally, other types of authenticators such as smartphone-based solutions could be used in an infrastructure that leverages multiple biometric modalities. This infrastructure would also need to consider the use of biometric scanners at facilities versus the use of ones on patients' smartphones. Regardless of the infrastructure used, privacy and security remain essential preconditions. Some examples for an infrastructure—which would need to be further assessed, developed, and tested—include the following:

Single modality, standardized: Health care organizations and technology developers could agree to standardize a portion of the template for a single modality. This would enable facilities to match on that standardized portion along with other data, such as demographic information. Security experts would need to mitigate the potential for disclosure of the standardized portion or the algorithm used to develop it. The use of a single, standard modality may also reveal other challenges, as has happened in similar approaches attempted internationally.[61]

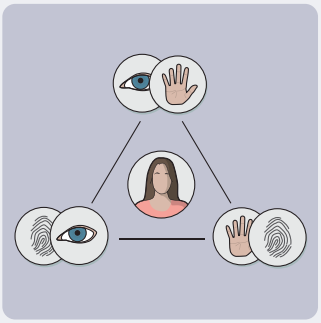
Continued on next page



Single modality, engine shared: Each biometric vendor could make available its matching engine, either by providing it to other organizations to embed in their system or via an application program interface accessible via the internet. Under this approach, the manner in which each matching engine functions would not be disclosed; rather, each engine would operate as a black box. The exchange of information would require significant privacy protections in case the information were intercepted.



Multiple modalities, repositories: If multiple independent repositories were created, they could be used by health care organizations and could collect and aggregate biometric information from multiple modalities within the same person's record. Some organizations could scan two or three different modalities and therefore be able to associate all with a patient in the database. In other cases, the demographic data would be clear enough to enable a match, which then would associate a new modality with the record. Organizations would then be able to use their preferred modality for identification. The repositories could provide a unique identification number based on the biometric, or simply a binary match versus no-match response when contacted by facilities.



Multiple modalities, query system: Each health care facility could adopt whichever modality it chooses, then use a combination of demographic data and biometric-based queries to other organizations to find matches. Through this query-based system, each health care facility would ask other establishments for information until it can confidently associate one modality received from another institution with the modality template that it has on file. The establishment of health information networks to help organizations share data—as envisioned by ONC—can serve as hubs to reduce the number of queries needed.

Prerequisites for unique identifiers to work for matching

Unique identifiers can greatly improve matching because they unambiguously identify each individual and therefore could—theoretically and if perfectly implemented—achieve close to 100 percent accuracy. However, unique identifiers face significant limitations. For example, alphanumeric identifiers are susceptible to typos if entered manually and without robust checksum digits, and to being forgotten by the patient. Also, biometric and other technology-based identifiers may require changes to workflow and the purchase of infrastructure by health care facilities.

Regardless of the approaches taken, these solutions can improve matching rates only so long as the following conditions are met:

- The identifier can be used for matching between facilities, not only within a facility. For example, even if every health care facility agreed to use facial recognition scans for identification, the scan should be computed into a data element (such as an alphanumeric code) in the same way by all scanners. Otherwise, the data elements used to document the scan would not be the same and, therefore, not usable to match patients between institutions.
- Software developers incorporate these solutions—using some level of shared standards—and appropriate privacy safeguards into their technologies.
- Health care providers are willing to implement the solution, which includes purchasing any needed hardware (such as a biometric scanner), training staff on its use, and incorporating it into the patient registration workflow.
- Patients are able and willing to use the identifier. For example, if biometrics are used, patients should be amenable to having that biometric scanned or captured upon registration and be confident that the data are secure. Similarly, patients should be able to use the technologies; for example, individuals who are less technologically adept may not be able to use a smartphone application as an identifier.

Key findings on unique identifiers

To evaluate whether a unique identification system could be established, Pew heard from patients, interviewed health care providers, examined the literature, and spoke with experts. Although unique identifiers are promising, several key challenges emerged.

Patients prefer biometrics over other unique identifiers

Of all the solutions tested, patients interviewed in focus groups overwhelmingly preferred the use of a unique identifier to improve patient matching, with very few individuals expressing reluctance. Participants said that a unique identifier would decrease medical mistakes, give clinicians a more complete picture of their health, and be more secure than demographic data.

Participants were asked about different forms of unique identifiers—including smart cards and usernames—and overwhelmingly supported the use of biometrics as the identifier. When given various options, 70 of 95 participants listed biometrics as their first preference for a unique identifier, with nearly all participants ranking it within their top two choices. Participants expressed that biometrics would help even in emergency situations for unconscious patients, would not need to be remembered by individuals, and would be more accurate and secure than other approaches. Participants also indicated an increasing familiarity and comfort with use of biometrics, particularly fingerprint scans.

Participants did not favorably view a unique number or password, as these would need to be remembered or brought to the health care facility. A number was also perceived as easier to steal and therefore less secure. Participants quickly dismissed the idea of smart cards—wallet-sized cards with microprocessors that would contain identification information—as they could be lost, stolen, or forgotten.

Health care providers question completeness

Health care providers interviewed generally welcomed the use of unique identifiers but expressed several concerns. First, many individuals and organizations probably would not adopt or implement unique identifiers at the outset, which would significantly inhibit their utility for early and possibly later adopters. As a result, government—particularly CMS—would probably need to mandate or encourage their use. Executives indicated that patient comfort with biometrics in consumer-related applications—such as to unlock devices or at airports—could encourage participation and that photographing individuals is becoming more prevalent in health care settings. Nevertheless, some executives worried about patient resistance with using biometrics as invasive.

Second, the health care providers indicated that biometrics probably represent the most valid and accurate method for identifying individuals but that this approach cannot be effective until standards exist for documenting the information, agreement is reached on the modalities to use, and deploying the technology becomes more cost-effective. As with a unique patient identifier, a biometric would be an additional data attribute to feed into, not replace, current matching processes.

Third, many health care organizations have already implemented biometrics for staff to, for example, enable easy and reliable access to devices that dispense medications.

Finally, executives at facilities that treat large undocumented populations indicated that many of their patients may hesitate to seek care at organizations that use unique identifiers—especially in the current political climate.

Additional considerations and findings

- *Biometrics emerging:* Biometrics are increasingly sophisticated, are embedded into consumers' daily lives, and typically can be used for identification without changing or being forgotten. Therefore, biometrics represent a key opportunity for use as a unique identifier in health care settings. Using biometrics, though, requires significant protections for the information and low-cost ways to adopt scanning technology in hospitals and clinics.
- *Lack of agreed-upon standards for the use of biometrics:* For biometrics to be leveraged as a nationwide identifier, hospitals and technology developers must agree to a process and set of standards for their use. The Trusted Exchange Framework and Common Agreement (TEFCA) from ONC may offer an opportunity to begin identifying standards, fostering discussions of their use, and fostering adoption. Through TEFCA, health care stakeholders could agree to a common set of standards and infrastructure to exchange data. Although TEFCA addresses interoperability writ large, a focus on matching—and biometrics specifically—could help build momentum and agreement across different stakeholders, including the patient privacy community, to prioritize this approach.
- *Authenticators could support a federated identity model:* Biometrics, smartphones, and other approaches can also be used in combination through a federated identity model. In this approach, which several experts interviewed suggested, multiple organizations or technology developers could aggregate different authenticators for an individual. For example, one organization could use different methods to combine all known identity information on a patient from every health care organization that sees the individual. Then, those organizations would agree to various standards and protocols to share identity information among them.

These organizations would build profiles for each patient, with matching challenges reduced as more data were received over time.

- *Political challenges with a federal unique identifier:* Adoption of a unique identification system could face challenges because of restrictions on the federal government funding such a solution. This restriction could inhibit the use of an agreed-upon unique identifier by patients who receive government benefits, such as through Medicare.
- *Use of Medicare identifiers does not resolve challenges:* The deployment of new Medicare identifiers to replace SSNs could provide some individuals with a unique identifier, especially because the Medicare population is highly stable with very limited switching to other plans. But several challenges persist. First, only the Medicare population will have these identifiers; for their use outside of Medicare, agreement would have to be reached about how to assign nonbeneficiaries this number and manage the system to retain the identifier when switching health plans. Second, even for the Medicare population, their records prior to enrollment would not be linked with the number. Third, the Medicare identifier could be stolen and used fraudulently—just like SSNs.

Potential next steps to consider on unique identifiers

Several opportunities exist to advance a unique identifier system, albeit only with widespread actions and support from across the health care system.

First, although not a prerequisite to private-sector action, addressing the statutory prohibition on funding for a unique patient identifier could foster progress. Congress should evaluate whether it should remove or amend this prohibition, even if the federal government will not establish a unique identifier, to encourage agencies to engage with the private sector and advance solutions.

Second, biometrics represent a promising approach for a unique identifier, though they could also be used along with other technologies—such as smartphone applications or cards for those patients who opt for an alternative approach. Biometrics are becoming increasingly common for various consumer purposes and even used by many consumers daily with their smartphones; biometrics and smartphone-based approaches could be similarly leveraged in health care. However, using biometrics for matching across organizations requires identifying and adopting standards and a nationwide agreed-upon infrastructure on how to leverage different modalities.

Therefore, health care industry leaders—including technology developers and health care providers—should evaluate the standards needed for the use of biometrics and other authenticators and agree to a nationwide infrastructure to support this effort. Implementation of TEFCA offers an opportunity to identify and develop those standards and infrastructure, included through a federated model in which different health networks are able to aggregate and share identifying information for the purposes of matching.

Regardless of the infrastructure selected for unique identifiers or similar approaches, developing and deploying such a system is not feasible in the short term. Identifying standards, establishing an infrastructure, obtaining broad health care support, using methods to protect privacy, and implementing the approach will probably require years of effort by technology developers and health care organizations.

Although the building blocks to using biometrics and other unique identifiers should be put in place as part of a long-term solution, they are unlikely to solve patient matching in the near future.

Opportunity 2: Patient-empowered solution

Health care facilities—and the technologies they use—typically have the responsibility to match records, with little to no direct involvement of the patient. Meanwhile, patients are increasingly gaining access to their health data, such as via online patient portals.

Efforts to improve matching may be able to leverage patients' ability to engage in their health care by giving them a more active role. Such an approach would represent a paradigm shift in matching, but it may face challenges in ensuring widespread adoption and utility for different patient populations—such as elderly, disabled, and low-income individuals.

To assess that concept, Pew contracted and collaborated with the RAND Corp. to evaluate different approaches to involving patients in matching.[62] RAND conducted a literature review, interviewed experts, and convened an advisory panel to identify different options for a patient-empowered matching strategy and criteria used to analyze each approach. The research identified several options, which ranged in the degree to which the patient would be involved. Some approaches included minimal patient involvement—patients could, for example, permit their pictures to be taken—while others included a more hands-on role for the individuals, including having each patient aggregating all his or her health data in one location or obtaining a voluntary unique patient identifier.

The research identified several criteria to evaluate each solution, including the degree to which it would improve match rates, the likelihood of patient adoption and use, and the feasibility of implementation.

In a report released in August 2018, RAND recommended a patient-empowered approach for matching involving two main components: validating patient information and a smartphone application, which would then be used together once developed.

Verification of patient information

The first stage of the RAND recommendation proposes the use of verified information—particularly mobile phone numbers—to enhance matching. Under this approach, patients, for example, could receive a text message to their phones that would require a response. This process would verify that the phone number was entered correctly and is associated with the patient. Hospital staff and technology companies could soon establish phone number–verification workflows, for example, as part of the check-in process. Although the CommonWell Health Alliance found minimal uptake in its attempts to encourage registrars to validate information, those efforts involved many changes to workflow. Implementing this single change in isolation may prove less burdensome on workflows, though facilities may need to invest resources to incorporate verification.

Phone number verification would help address some causes of matching errors—such as typos—and enhance the utility of phone numbers in matching algorithms. However, phone number verification is still limited in its ability to improve matching because patients may change numbers, share them with other individuals, or fail to effectively respond to requests for verification. Efforts underway by some organizations—such as the CARIN Alliance, a multisector group of organizations that are advancing patient access to data—may help advance identity assurance, which could support greater verification of attributes.[63]

Smartphone-based solution identified

The second stage of the solution involves the creation of smartphone applications, which would use similar standards so that each EHR could more easily receive data from different mobile devices. Patients would use their

devices to transmit several key pieces of data to EHRs to improve matching. The data would involve the following: core demographic information that the patient can regularly update as needed and ensure is accurate; unique identifiers that the patient may have, such as a driver's license number; and a verified phone number.

This information, in aggregate, would improve matching by ensuring that health care organizations can match records based on accurate, up-to-date data, including identifiers unique to an individual. Both patients and health care organizations would adopt these applications because they would help streamline the registration process. For example, these applications could serve as virtual clipboards to replace the patient manually filling out demographic data on paper forms when arriving at facilities. Instead, a patient would enter this information only once, which would then be reused and sent electronically in lieu of at least some data needed on paper forms.

The final stage of the RAND proposal involves developing additional functionalities in the smartphone applications to enhance utility and adoption.

Figure 1

Patient-Empowered Matching May Involve Use of Smartphones

Verified data, information sent directly by patients

Increased use of smartphones could allow patients to improve match rates for their data. For example, patients could verify their demographic data by responding to a text message to confirm that their phone number was entered correctly. With the development of certain applications, patients could also enter their data on their phones and have it sent to health care providers via QR codes or other mechanisms.

Key findings on smartphone-based approach

In addition to commissioning RAND to evaluate a patient-empowered approach, Pew also spoke with patients via focus groups and interviewed health care providers to evaluate their perspectives.

Patients worry about security and utility of smartphones

The vast majority of patients interviewed in focus groups preferred the use of biometrics for matching, but some individuals welcomed the use of smartphone applications to reduce the paperwork that they would be required to fill out in waiting rooms. Some individuals also indicated that they already conduct many personal activities—such as financial tasks—on their phones, and they welcomed also having access to health-care-related data.

However, many participants dismissed the use of smartphone applications as a viable option for patient matching because of the perception that it would not be effective for many people—such as seniors and low-income individuals—and in emergency situations. Participants said that seniors, even those who have smartphones, may not be able to effectively operate an application or may face challenges reading the text. Despite this perception from focus group participants, the Pew Research Center found in 2018 that two-thirds of the Baby Boom generation (born between 1946 and 1964) own smartphones.[64] Similarly, researchers from the University of Southern California examined data on 421 homeless adults and indicated that 94 percent of them in 2017 owned a cellphone, though most had experienced high phone and phone number turnover in the preceding three months. More than half of the homeless adults owned smartphones.[65] Cellphones—even if not smartphones—still may be able to be used to verify the number. Patients in focus groups also expressed strong concerns about the prospects of smartphones being hacked or lost.

Providers welcome use of smartphones but question robustness

Most health care providers interviewed indicated that the use of smartphones could have promise by giving patients more control—especially as technology giants, like Apple, have promoted patient-controlled health records and because of broad adoption of smartphones.

However, health care providers interviewed expressed the opinion that several challenges remain, including uneven uptake (such as ensuring participation among the elderly population); patients putting in incorrect information; device security gaps; potential inability to provide proxy access to caregivers; and the possibility that individuals would create duplicate records for themselves.

Additionally, the transfer of information from patients' smartphones to EHRs may introduce challenges, including the need for technology—such as application program interfaces that can write data into the system—to enable the flow of data, and infrastructure to support wireless communications between the app and health care facilities. Similarly, health care executives interviewed wondered whether the introduction of new data into the EHR could provide an opportunity for malicious software to be incorporated.

Additional considerations and findings

- *Increased emphasis on patient empowerment:* The health care industry has increasingly focused on enabling patients to take a more active role in their care—a goal that a smartphone-based solution would help advance. Patient empowerment even has bipartisan support. The Trump administration has prioritized efforts to ensure that patients get their health information, while former Vice President Joe Biden has spearheaded similar efforts focused on cancer.[66]

- *Not immediately effective for all populations:* Not all patients have or would be willing to use smartphone applications for exchanging demographic data. Similarly, not all patients—such as children—have existing unique identifiers or their own smartphones with which to validate a unique number. Despite this limitation, the use of smartphone applications can still help millions of patients, especially individuals with multiple chronic conditions and those who seek to be more involved and engaged in their care. Similarly, smartphone applications could evolve to incorporate different types of unique identifiers and leverage the information of caregivers, such as by matching on a parent's validated phone number while retaining that this information does not exclusively belong to the patient.

Pilot, standards key next steps on patient-empowered approach

To further evaluate and develop a smartphone-based approach to empower patients to enhance matching rates, several steps are necessary.

First, independent of the creation of smartphone applications, technology vendors, health care systems, and ONC should evaluate the prospects of integrating phone number validation into workflows and conduct pilots to assess whether and to what degree matching improves. Based on the findings, ONC could further evaluate ways to encourage phone number validation through its policies and programs.

Second, interested smartphone-health-application developers, EHR vendors, health care providers, and other key organizations should host a series of meetings to refine the details of this concept so that a prototype application can be built. This refinement should include, for example, the standards to exchange information with EHRs and how the data would be used among systems for matching.

Third, those groups should work together to build a prototype application and conduct a series of pilots to further refine the technology. These pilots would, for example, identify and address workflow challenges within health care institutions to collect and use data from the application, assess issues that patients encounter when using the application, and evaluate the utility of this approach in improving match rates.

Fourth, the future use of this smartphone-based approach could evolve in several ways. One option is for these smartphone applications to evolve into more robust personal health records that aggregate patient data from multiple EHRs. In this approach, these applications would need to be able to pull information out of EHRs—not just push information to them.

Alternatively, existing smartphone applications that aggregate patient data—such as the one developed by Apple—could incorporate a matching function that passes identity information to EHRs. Currently, these personal smartphone-based health records pull information out of EHRs without pushing anything back to them. By incorporating this push function, personal health record companies could provide additional benefits to patients by reducing paperwork associated with clipboards while also helping health care facilities match records.

Even in the future, if many patients aggregate their own health information, matching between health care organizations will still be needed. Some individuals may not collect on their smartphones new health data every time they seek care, for example.

The use of smartphones continues to gain momentum and revolutionize how consumers—and patients—interact with many industries, including health care. The increased use of these devices and the health care industry's renewed emphasis on patient empowerment offer an opportunity to build on this interest to enhance one of medicine's greatest long-standing problems—the ability to link individuals with their records.

Opportunity 3: Demographic data standardization

Patient matching relies on the use of demographic data and can be affected by the specific information used and how it's formatted. For example, one system may document email addresses, which may be omitted from another system. Or some organizations may use a single field for a person's full name, while another may have three discrete fields for first, middle, and last names.

To address this variability, many organizations—including in different reports from the Bipartisan Policy Center and Audacious Inquiry, which investigated matching for ONC—have recommended standardizing data attributes and formats as a solution.[67]

Data elements collected

A 2015 study by Intermountain Healthcare found that the combination of certain data elements—such as using ZIP codes in conjunction with commonly captured demographics, such as last names—resulted in higher match rates. A subsequent 2017 study consisting of nine health care systems from different regions examined the availability of different data elements across locations and over time, finding that some information is increasing in prevalence. For example, the availability of email addresses increased from 9 percent to 54 percent from 2005 to 2014 and may have utility for matching.[68] This finding echoed 2011 recommendations from a federal health IT advisory committee to support the use of email addresses and other voluntary identifiers, such as biometrics, as potential patient matching attributes.[69] However, the researchers conducting the 2017 analysis found that recording Social Security numbers declined from 83 percent of the time to 50 percent. This finding reinforces that the use of these numeric identifiers is unlikely to sufficiently support matching in the future.

Although the use of increasingly documented data elements could provide additional information on which to conduct matching, they remain susceptible to the same limitations as the others, including typos and changing information.

Standardization of data elements

Many organizations have recommended standardization for each piece of information used for matching, but the utility of standardizing each data element had not been independently tested.

To conduct this evaluation, Pew and Indiana University's Regenstrief Institute collaborated to test the standardization of data in real-world records. Through this research, Regenstrief evaluated the match rates of records in four databases using a standard algorithm, standardized the data, and re-ran its algorithm to evaluate changes. The four databases—which contain tens of thousands of records each—are considered gold standard, meaning that they have been manually curated by Regenstrief to determine the true matches so that a denominator is known. Each of the four databases reflected one of the following uses: hospital-to-hospital matching; de-duplicating records in a public health registry; linking clinical data from a hospital registry to death files maintained by the Social Security Administration; and matching newborn laboratory data to a health information exchange.

The following fields and standards were used to evaluate standardizations. Each standard was chosen through an evaluation of different standardization options:

Table 2

Data Elements and Standards Examined to Improve Patient Matching

Data element	Applied standard/rules	Effect
Last name	Applied normalization rule from the Council for Affordable Quality Healthcare, a nonprofit alliance of health plans and trade associations	Removal of special characters (such as apostrophes) and suffixes, such as "Jr."
Telephone number	Formatted according to International Telecommunication Union Recommendation E.123	Converting numbers to the format (XXX) XXX-XXXX
Social Security number	Default and invalid values removed	Invalid values made blank
Date of birth	Date rules applied	Invalid dates made blank
Address	Applied U.S. Postal Service certified address standardization rules	Corrected errors that would make an address undeliverable by the U.S. Post Office and spelled out abbreviations, such as changing "blvd" to "Boulevard"

In addition to determining whether standardizing individual data elements improves matching, Regenstrief examined whether different combinations of standard data elements further improve matching.

The full findings from the research have not been published as of September 2018, but indicate that standardization of some demographic data shows promise for increasing the likelihood that records are matched.

Key findings on standardization

Based on the Regenstrief-led research, published literature, and interviews with patients and health care providers, several key findings emerged as to the utility of standardization.

Patients question whether all providers will adopt standardization

There is strong support among focus group participants for health care facilities to capture data in a standard way to improve patient matching. However, patients questioned whether all health care providers are likely to agree to standardization and the associated costs.

Providers have recognized value of standardization

Health care providers interviewed welcomed increased standardization without reservation, and many have

already invested in staff training to ensure that information is documented in the right fields (for instance, to put "Jr." separate from the last name). Some organizations have also restricted data sharing with external partners that do not meet minimum quality criteria for how the data are displayed. Health care providers indicated that both CMS and ONC can help ensure more effective standardization on a nationwide scale. For example, ONC—via TEFCA or EHR certification programs—can encourage standardization, or CMS could include these standards as a prerequisite in its payment programs.

However, health care providers interviewed underscored that standardization still does not solve all patient matching challenges such as typos, and it leaves opportunities for progress even if all data are standardized. Additionally, they indicated that the use of additional unique data types—such as mobile phone or driver's license numbers—can make more effective gains than standardizing each piece of information or improving the quality of existing data.

Additional considerations and findings

- *Limited standardization offers promise:* Standardization of some demographic elements can improve matching. The increases possible through data standardization can help link many records that otherwise might not be matched.
- *Emerging demographic data provide future opportunities:* In addition to standardizing certain common demographic data elements, attributes that appear increasingly to be captured, such as email addresses, could be used for patient matching.[70] At the same time, others that are decreasing in availability, like Social Security numbers, may become less useful for patient matching. Organizations should test the utility of new demographic data elements, such as email addresses, for matching purposes.

Next steps on standardization

Standardizing which data health care providers collect and how they format it is likely to provide improvements to matching on a nationwide scale, especially for organizations that cannot in the near term invest in new match technologies or approaches.

The research conducted by Regenstrief reinforces recommendations previously issued—that standardizing the formats of some demographic data (particularly address and last name) improves match rates.

Along with standardizing such data elements, technology vendors—including EHR developers—and health care providers should reach agreement on additional data elements to collect and use for matching, such as email addresses. The collection of email addresses can provide health care organizations with other benefits, such as for billing or granting access to patient portals. Future work should examine the accuracy of patient matching when nontraditional demographic attributes are used for matching.

Given that wide-scale adoption of the same standards and data elements would be needed to realize the utility of standardization, EHR vendors should prioritize the deployment of standardized fields to their customers. Standardization would also help obtain economies of scale in transitioning to standards where needed. Health care providers should ensure adoption and adherence to agreed-upon standards.

Further, government may have an increased role in helping ensure more robust nationwide adoption of standards and in helping the industry coordinate to select standards for demographic data. The Recognized Coordinating Entity (RCE), which ONC will select to help implement TEFCA, or other ONC programs could fill this role.

Opportunity 4: Referential matching

Incomplete or outdated demographic data in patients' records can prevent accurate matching. For example, an individual who moves will have different addresses over time in health care facility databases. And patients' names can change when they undergo a life event, such as marriage or divorce. Other ambiguities also exist in identity data. People can have multiple versions of their first names (nicknames, for example), individuals may reside at several addresses (such as if they have a winter home or beach house), and twins can have similar names and other data.

To address these challenges, one increasingly prominent approach for patient matching also relies on demographic data, but with additional information culled from multiple sources, typically from outside of health care. This approach—known as referential matching—leverages data from different sources to build a more complete profile of each patient that includes past addresses, common name spellings for the individual, and other demographic data that has changed over time.

For example, change of address information submitted by an individual to the U.S. Postal Service can help link a new and previous address for that patient. Referential matching vendors can pull this information into their systems so that if health care facilities have different addresses for an individual, the data can be compared to the profile created from multiple sources to determine whether they are referring to the same person. Other data sources include credit bureaus and commercial aggregators of identity information.[71]

Two predominant approaches exist for the use of referential matching. One involves using a referential matching for all patients. In effect, this approach replaces other matching techniques, such as probabilistic algorithms. The second approach involves using referential matching only for the hardest cases—where the existing, nonreferential matching system cannot confidently make a positive match. Health care organizations continue to use their existing matching systems for the more straightforward cases.

Figure 2

How Third-Party Data Could Improve Patient Matching

Pew Launched Referential Matching Group for Voter Registration

Given the promise of referential matching, this approach has generated significant interest in other industries, including voting. States face challenges in knowing that everyone on their voting rolls still lives in the state, along with identifying potential unregistered voters.

To address that challenge, Pew collaborated with states to launch the Electronic Registration Information Center (ERIC)—which aggregates data from many sources, including state motor vehicle licensee information—to conduct referential matching. This approach has helped states increase the accuracy of their voting rolls. As of July 2018, 23 states and the District of Columbia participated in ERIC.

Although promising for voter registration, this type of approach in health care is not entirely analogous. For example, using this approach for voting required the creation of a single center to house the data; no such center exists for health care today. Identifying one or more organizations to serve this role would be needed. Additionally, referential matching is not currently effective for children, which is not relevant for the voting-age population but is in health care. Solutions to this challenge would need to be addressed.

Referential matching has promise, key challenges

To evaluate the future role of referential matching to link patient records, Pew reviewed publicly available information, spoke with vendors that offer this service, and interviewed patients and other experts on the promise and limitations of this approach.

Patient concerns with referential matching

Based on a brief summary of referential matching, focus group participants expressed concerns with referential matching, particularly the use of data received from credit bureaus given a perception that their health and financial information could be mixed or that their health care providers or insurers would have access to their financial information (despite this concern, in current referential matching approaches, health information is not shared outside health care facilities, and only the identification information from financial institutions is used—not credit data). Patients also expressed concerns that credit bureau information is not accurate, and they feared for the security of the data, given news stories about hacks. They also expressed concerns about the information from the U.S. Postal Service not being current.

Some providers raised questions

Individuals from some organizations emphasized that other industries also conduct identity management and that using data and resources from outside health care can provide benefits.

However, the executives also expressed reservations with this approach, noting that the third-party data sources used for referential matching are not always accurate. Some use data from the Social Security Administration,

though this information can be inaccurate—for example, by incorrectly listing that an individual is deceased. Additionally, the data contained are not necessarily unique to a single individual; therefore, errors can still occur. However, this may be less likely with referential matching than with other approaches, given the availability of additional data sources to address inaccuracies.

Finally, logistical challenges might also hinder adoption, including the perception that these solutions are costly and that business associate agreements would need to be in place. However, a developer of a referential matching solution indicated that the company's services would reduce overall costs from having to manage duplicate and incorrectly merged records when other approaches are used and that strategies can be implemented to address concerns about business associate agreements.

Additional considerations and findings

- *High reported match rates:* Referential matching has significant promise. One company that sells this service reports having a 98 percent match rate, which is among the highest reported.[72] However, this match rate has not been independently verified. Such a study should compare the match rate of referential matching against other matching algorithms using real patient data, including errors, to determine the improvement.
- *Gaining traction in the industry:* As of early 2018, the company with a reported 98 percent match rate self-reports working with organizations that cover up to 20 percent of the U.S. population—though this may not cover every encounter those people have with a health care provider.[73] This approach is also likely to continue gaining traction among health information exchanges, technology developers, and large health systems, which would further benefit additional patients and ensure that more of each individual's records are accurately matched. Given this trajectory, referential matching may—on its own—be adopted broadly, though additional steps might be needed to ensure matching across organizations as opposed to using this approach for each organization to manage only its own patient record database.
- *No improvement for matching among certain populations, especially children:* Many of the data sources used for referential matching do not contain information on children, homeless individuals, or other subpopulations. As a result, the added benefits of third-party data are unrealized, where standard demographic-based matching would still be used. Along with representing a significant portion of the U.S. population that regularly obtains health care services (such as annual physicals, vaccinations, athletic injuries), pediatric patients also face unique challenges with matching.
- *Opportunities to address matching for children:* To solve challenges using referential matching, several approaches have potential. For example, referential matching vendors could seek access to other data sources that contain pediatric populations, though enhanced scrutiny would probably occur, given the sensitivity of information on children. Another approach may involve using the information of patients' guardians, so that accurately matching the parent or guardian would serve as a surrogate for matching the pediatric patient.
- *National referential matching service proposed:* Referential matching could offer an opportunity to create a series of services for cross-organization linking of patient records. Under this approach, multiple health care organizations—such as hospitals, pharmacies, or health information exchanges—would all use the same referential matching service. By doing so, each organization would have its patient list mapped to the same identifier provided by the matching service; that identifier could then be used for matching between organizations.[74] They could further obtain the collective benefits of also being able to leverage any identifiers—such as biometrics or drivers' license numbers—collected by the other organizations and stored in the matching service. Each referential matching service would effectively build a profile of each patient that aggregates both demographic information and these identifiers.

- Standards and processes would need to be put in place for each of these services to communicate with one another and refine their profiles to support a multivendor solution. Through this approach, health care organizations might achieve the reported referential matching rates while gradually incorporating emerging technologies such as biometrics. The development of a nationwide strategy for interoperability (e.g., via TEFCA) may offer the opportunity to establish this model by encouraging adoption of technologies—such as referential matching—that achieve high match rates within each health information network.

Potential next steps on referential matching

Ultimately, using referential matching seems promising for improving match rates for many patients. However, questions remain with certain key segments of the population, such as children. Also, the infrastructure—both at a policy level and adoption in the private sector—has not yet been broadly built and deployed to use referential matching across organizations.

Several policy and research steps can be taken to refine and advance referential matching.

First, referential matching vendors should work with researchers on an independent analysis to understand the match rates associated with this method. The analysis should rely on real patient information to be able to fully leverage the data sources on which referential matching algorithms rely. The analysis should ultimately provide an assessment of how much referential matching improves rates beyond standard algorithms that lack new data sources.

Second, referential matching vendors and policymakers should examine whether other data sources or techniques should be used to help achieve even greater match rates—especially for populations such as children who do not obtain an additional benefit from this approach.

Third, policymakers, referential matching vendors, technology developers, and health care providers should consider deploying a strategy that uses referential matching both within and across health information networks. This strategy, which could be implemented via TEFCA, could create a gradual path toward higher match rates in the near term while supporting the adoption and use of new technologies and identifiers.

Ultimately, addressing the questions around referential matching and considering its use as a service across many organizations can help inform discussions on its role in a nationwide strategy and the gaps that remain after using this approach.

Nationwide strategy concepts

The success of the aforementioned approaches to matching—from the use and standardization of demographic data to biometrics—relies on the identification of standards, the use of a shared infrastructure, and agreement across health information technology developers, health care facilities, and other key organizations to take implementation steps. At the same time, some steps to improve patient matching can occur in the short term, while others would require refinement and coordination across many public- and private-sector stakeholders to enhance match rates even further. To address these short- and longer-term opportunities, a nationwide strategy is needed.

Pew—in conjunction with John Halamka, chief information officer of Beth Israel Deaconess Medical Center—hosted a 2017 meeting with approximately two dozen patient matching experts from government, technology vendors, health care systems, and other organizations to identify the key characteristics needed for a nationwide strategy to address the disparate methods and practices used to match patients across health care facilities. Findings from the meeting were published in the *Journal of the American Health Information Management Association* in July 2018 and are summarized here.[75]

Need for a nationwide strategy

The meeting and subsequent conversations with experts identified several reasons to have a nationwide strategy for patient matching.

First, each health care facility uses different methods, technologies, and practices to match records internally. Those systems may not, though, help facilitate matching across organizations. For example, a hospital that uses palm vein scanners to assist with patient registration may not be able to use that same technique with organizations that lack that technology or use different devices without a common standard.

Second, matching is fundamentally an activity that occurs among unaffiliated organizations—often across state lines. Therefore, a strategy is needed to help these organizations link patient records even when doing so occurs infrequently.

Third, matching involves many organizations from different industries, both health care and technology. Ensuring that these industries—and not just individual organizations—coordinate effectively requires a more robust strategy.

Fourth, as matching requires the identification and implementation of standards, a nationwide approach is needed to identify the appropriate criteria and encourage their adoption.

Finally, the technologies and approaches used for matching are likely to evolve. A nationwide strategy could help incorporate new approaches and ensure that they seamlessly integrate with existing efforts.

Need for a single organization to steward matching progress

As part of the nationwide strategy, experts convened by Pew identified the need for a single stakeholder-driven, trusted organization to oversee and advise on ways to improve patient matching, develop and implement policies within a standards-based infrastructure, and incorporate new technologies and promising approaches as they emerge.

This entity could help recommend ways to make progress in the short term, such as via more robust demographic standards. It would also identify and encourage adoption of certain standards—such as on biometrics or use

of smartphones—by health care organizations and technology developers to make more robust progress on matching that would require additional time and investments.

Such an organization may be in development via TEFCA. ONC has indicated that it will task a single organization, called the Recognized Coordinating Entity (RCE), with establishing policies and overseeing the exchange of data among these networks.[76] The RCE could serve as a platform to serve as this trusted organization, develop short-term guidance on improving matching, and identify standards and an infrastructure for even more robust matching.[77] ONC should ensure that the RCE can serve this function.

Absent the RCE prioritizing matching, health care organizations, technology vendors, and other private-sector groups should collaborate to launch an independent organization to serve as this trusted entity.

Other factors key to a nationwide strategy

Along with the identification of a single organization to help shepherd improvements in matching, experts at Pew's July 2017 meeting identified several other factors needed for long-term progress.

- *Private-sector focus:* As health care providers and technology developers bear primary responsibility for matching, the organizations should drive efforts to make progress. At the same time, government—including ONC and CMS—can help support and adopt recommendations and approaches generated by the private sector.
- *Reliance on standards:* A nationwide strategy should be standards based, which could include establishing a minimum demographic data set, leveraging existing standards as suggested by federal advisory committees or standard bodies, and building on market innovations.
- *Flexibility:* Given that health care organizations vary in the types of technologies they use and their ability to adopt new approaches, a nationwide strategy should be flexible to accommodate this variation.
- *Common agreement:* A universal policy is needed to define how and what data can be used for matching, along with necessary privacy rules and policies to facilitate matching and exchange. ONC's draft TEFCA also includes a common agreement that defines the terms and conditions for exchange among participants and could serve this role once fully implemented.
- *Public disclosure:* As the success of a nationwide strategy relies on ubiquitous implementation by health care organizations and acceptance by patients, public disclosure of privacy and other policies can help assuage concerns and foster transparent feedback from these stakeholders.
- *Patient empowerment:* A nationwide strategy should empower patients to engage and act on their privacy preferences, including input on when to share or opt out of records exchange. Patients should have clear information on how their data will be used, the benefits and drawbacks of sharing or withholding data, and when exchanging information can legally occur among providers without explicit consent. Policies should also exist for individuals to correct or supplement information that can be used for matching.
- *Trusted identity:* Increased assurance that patients are who they say they are is also a critical component to improved matching and in preventing individuals from using other people's information. This can be accomplished by verifying identity information, such as through third-party data sources to provide assurance that a specific individual lives at the provided address, or with two-factor authentication.

- *Clarity on state laws:* Individual states also have their own patient privacy and data exchange policies, as federal regulations only establish minimum requirements that some states expand upon. Clarifications and consistent application of data-sharing practices across states could facilitate organizations' willingness to implement a nationwide strategy and foster development of a universal, national policy. ONC's draft TEFCA highlights some of these challenges, such as policies restricting the sharing of certain information among Prescription Drug Monitoring Programs in different states and the level of patient consent required to share data, which hinder data exchange, including for matching. The trusted entity could help harmonize state policies and address variations among states.
- *Legal protections:* Increased sharing of data—including demographic information or other personal identifiers—also raises potential risks around unintentional disclosure of information even when best practices are followed. Legal protections and safeguards may be needed to mitigate risks and concerns.

Conclusion: Near- and long-term opportunities exist to advance matching

The current state of patient matching has left many records unmatched, which can lead to patients and clinicians lacking the information they need to make informed health care decisions, and that contributes to avoidable costs. The status quo—even with small, incremental progress—is not enough to address and resolve matching.

Some opportunities exist to improve patient matching and create more complete medical records, so that patients' diagnoses, medications, and other key information are accessible regardless of where they were documented.

Near-term opportunities to advance matching

In the near term, government, health information technology vendors, and hospitals can take several steps to make progress while a longer-term solution can be developed, agreed upon, and deployed. Specifically:

- *Recommendation 1: Clarify funding:* Congress should examine whether to maintain the funding ban on the Department of Health and Human Services implementing a unique health identifier, and it should encourage federal agencies to collaborate with the private sector on solutions. Although a government-issued alphanumeric identifier is unlikely to resolve the matching challenge, the ban has limited government actions to collaborate with the private sector on solutions.[78] CMS should also examine how it can take incremental steps to improve matching, such as setting goals and requirements for providers participating in Medicare and Medicaid, and examining whether the private sector could leverage government efforts to replace Social Security numbers on identification cards.[79]
- *Recommendation 2: Agreement on data elements and standards:* Technology vendors—including EHR developers—should agree on additional data elements to collect and use for matching—such as email addresses—and common standards for depicting the information. Such agreement will not only provide additional data for matching, it would also generate meaningful improvements to match rates. ONC can coordinate with the industry, including via the RCE once selected, to identify and encourage adoption of these standards.
- *Recommendation 3: Verification of data:* Health care providers and technology vendors can embed phone number verification or other techniques to ensure information provided by patients is accurate. This verification will provide greater assurance of the accuracy of demographic data for matching. A phone number, in particular, is a persistent and unique data element. Verification would prevent typos and other challenges to matching, and it would not require substantial technological advances, though health care organizations would need to implement workflow changes and train staff accordingly.
- *Recommendation 4: Assess privacy:* ONC, other government agencies, and technology developers should also continue to examine the privacy and security implications of various approaches used to advance patient matching. Ensuring broad patient support requires addressing both real and perceived concerns about privacy and the use of individuals' information.
- *Recommendation 5: Examine referential matching:* Finally, health care organizations—including health information networks—should consider incorporating referential matching into their processes, given that this approach has generated among the highest match rates currently published. However, several key questions persist, which vendors of this approach should address. Vendors should ensure that an independent analysis is conducted and evaluate how to improve the use of referential matching for pediatric patients. ONC should also consider how to incorporate referential matching on a national scale, including through the trusted exchange framework.

Steps to identify a long-term vision and progress

Making more robust, long-term progress on patient matching requires the development of an infrastructure to support a nationwide strategy. To implement such a system:

- *Recommendation 6: Establish a trusted entity:* A single, national organization should exist to help advance the identification and adoption of standards to improve patient matching as technology develops. Such a system would ensure that standards exist for the use of biometrics and other approaches that could significantly enhance match rates. The implementation of TEFCA could provide an opportunity for long-term progress through a commitment of ONC and the RCE to govern that strategy. Alternatively, the private sector—including hospitals, technology developers, and patients—can create an entity to steward matching going forward.
- *Recommendation 7: Leverage smartphones:* Given the increased role that smartphones have in people's everyday lives, technology developers and health care organizations should collaborate with patients on how to leverage these devices to improve matching. Next steps include the identification of necessary standards, the development of a prototype smartphone application, and the piloting of this approach in select health systems. The standards identified should ensure that applications can run on different types of smartphones and cover the development of guidelines for protecting patient information and for how data are used. The use of smartphone applications for matching may evolve into personal health records or be embedded into other applications that extract data from EHRs. Either outcome, though, requires the development of standards and testing in clinical settings.
- *Recommendation 8: Identify infrastructure:* Finally, government, technology developers, health care organizations, and other stakeholders should collaborate on how to establish a federated model where many types of authenticators—including biometrics and smartphones—are able to be used along with demographic data. Such a system could rely on a small number of identity-management organizations, which could include health information networks, aggregating data to build patient profiles, and sharing information among one another. Such a model—independently proposed by multiple identity-management and referential matching vendors—emerged as a possible infrastructure for multiple approaches examined by Pew. Its success would also probably rely on a trusted entity to help manage the infrastructure; the identification and use of standards; and provisions to protect patient privacy. This approach would help create a process to optimize the use of demographic data such as through referential matching, while being able to use that same infrastructure to begin collecting authenticators—including biometrics—as they are used. In fact, that federated approach is a central pillar to recommendations from the National Institute of Standards and Technology on how to manage identification more broadly, though many factors specific to health care would need to be addressed.[80]

Given the various opportunities possible to improve matching, health care providers, technology developers, government, and patients should collaborate to develop a roadmap on how to implement and stage these and other approaches to better link records.

Improvements to matching are essential to realizing the potential of an interoperable health care system where patients and clinicians have data when and where they need them. Health care organizations, technology developers, and government have key steps that they can take to generate progress in the near term and help build a more robust infrastructure to support longer-term progress. Implementation of these steps can help better link patient records, giving individuals complete and comprehensive information on their care to improve quality and reduce costs.

Endnotes

1 Bipartisan Policy Center, "Challenges and Strategies for Accurately Matching Patients to Their Health Data" (2012), http://cdn.bipartisanpolicy.org/wp-content/uploads/sites/default/files/BPC%20HIT%20Issue%20Brief%20on%20Patient%20Matching.pdf.

2 Genevieve Morris et al., "Patient Identification and Matching Final Report" (2014), https://www.healthit.gov/sites/default/files/patient_identification_matching_final_report.pdf.

3 Ibid.

4 Verato Inc., "Verato Healthcare Solutions for Providers: Maximize Electronic Health Record (EHR) Value and Interoperability With a Revolutionary New Patient Matching Engine" (2016), https://www.verato.com/wp-content/uploads/2016/05/HealthcareSolutionsforProviders.pdf.

5 The Sequoia Project, "A Framework for Cross-Organizational Patient Identity Management: Draft for Public Review and Comment" (2015), accessed June 5, 2017, https://sequoiaproject.org/wp-content/uploads/2015/11/The-Sequoia-Project-Framework-for-Patient-Identity-Management.pdf.

6 College of Healthcare Information Management Executives, "Summary of CHIME Survey on Patient Data-Matching" (2012), https://chimecentral.org/wp-content/uploads/2014/11/Summary_of_CHIME_Survey_on_Patient_Data.pdf.

7 Beth Haenke Just et al., "Why Patient Matching Is a Challenge: Research on Master Patient Index (MPI) Data Discrepancies in Key Identifying Fields," *Perspectives in Health Information Management* 13, Spring (2016): 1e, http://perspectives.ahima.org/why-patient-matching-is-a-challenge-research-on-master-patient-index-mpi-data-discrepancies-in-key-identifying-fields.

8 Beth Haenke Just and Karen Proffitt, "Do You Know Who's Who in Your EHR?" *Healthcare Financial Management* 63, no. 8 (2009): 68-73, https://www.justassociates.com/application/files/2514/9124/7591/HFM_August_2009_Do_You_Know_Whos_In_Your_EHR.pdf.

9 Office of the National Coordinator for Health Information Technology, "Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap," accessed June 12, 2017, https://www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperability-roadmap-final-version-1.0.pdf.

10 Black Book Market Research, "Improving Provider Interoperability Congruently Increasing Patient Record Error Rates," news release, April 10, 2018, https://blackbookmarketresearch.newswire.com/news/improving-provider-interoperability-congruently-increasing-patient-20426295; Steve Kotyk, ARGO Healthcare Solutions, "Defining the (Enterprise) Master Patient Index (E)MPI: What's the Problem?" (patient matching presentation at the 2018 Maryland Health Information Management Association Annual Meeting, Rockville, Maryland, May 18, 2018), https://www.registrationconnex.com/wp-content/uploads/2018/05/Patient-Matching-1.pdf; Selena Chavis, "Patient Matching: The Saga Continues," *For the Record* 30, no. 2 (2018): 10, http://www.fortherecordmag.com/archives/0218p10.shtml.

11 Just et al., "Why Patient Matching Is a Challenge."

12 Just and Proffitt, "Do You Know Who's Who?"

13 Just Associates, "Studies in Success: Duplicate Records Compromise a Costly EHR Investment," accessed July 20, 2018, http://www.justassociates.com/application/files/5415/1707/3257/Just_Childrens_Dallas_Testimonial_Online.pdf.

14 Morris et al., "Patient Identification and Matching."

15 Just et al., "Why Patient Matching Is a Challenge."

16 Black Book Market Research, "Improving Provider Interoperability."

17 Government Accountability Office, "Identity Theft Services: Services Offer Some Benefits but Are Limited in Preventing Fraud" (2017), https://www.gao.gov/assets/690/683842.pdf.

18 Richard Hillestad et al., "Identity Crisis: An Examination of the Costs and Benefits of a Unique Patient Identifier for the U.S. Health Care System" (2008), http://www.rand.org/pubs/monographs/MG753.html.

19 Morris et al., "Patient Identification and Matching."

20 Just et al., "Why Patient Matching Is a Challenge."

21 Giuseppe Lippi et al., "Patient and Sample Identification: Out of the Maze?" *Journal of Medical Biochemistry* 36, no. 2 (2017): 107-12, http://dx.doi.org/doi:10.1515/jomb-2017-0003; Harris Health System, "Harris County Hospital District Puts Patient Safety in the Palm of Your Hand," accessed July 20, 2018, https://www.harrishealth.org/es/access-care-hh/Pages/HCHD-puts-patient-safety-in-the-palm-of-your-hand.aspx.

22 Grant D. Landsbach, "Study Analyzes Causes and Consequences of Patient Overlay Errors," *Journal of the American Health Information Management Association* 87, no. 9 (2016): 40-43, http://bok.ahima.org/doc?oid=301860#.Wr3IhK6nGpo.

23 College of Healthcare Information Management Executives, "Summary of CHIME Survey on Patient Data-Matching."

24 Adam Culbertson et al., "The Building Blocks of Interoperability: A Multisite Analysis of Patient Demographic Attributes Available for Matching," *Applied Clinical Informatics* 8, no. 2 (2017): 322-336, https://doi.org/10.4338/ACI-2016-11-RA-0196.

25 Meredith Dost and Kyley McGeeney, "Moving Without Changing Your Cellphone Number: A Predicament for Pollsters," Pew Research Center, Aug. 1, 2016, http://www.pewresearch.org/2016/08/01/moving-without-changing-your-cellphone-number-a-predicament-for-pollsters/.

26 American Health Information Management Association, "Fundamentals for Building a Master Patient Index/Enterprise Master Patient Index (Updated)," *Journal of the American Health Information Management Association,* updated September 2010, https://engage.ahima.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=ca53ccdc-60bb-4320-a014-8652894a588e.

27 The Sequoia Project, "A Framework for Cross-Organizational Patient Identity Management."

28 Ibid.

29 CommonWell Health Alliance, "Overview of CommonWell Services," updated February 2017, http://www.commonwellalliance.org/wp-content/uploads/2014/10/CommonWell-Concepts.Feb_2017.final_.pdf.

30 Office of the National Coordinator for Health Information Technology, "Patient Matching Algorithm Challenge," accessed July 24, 2018, https://www.patientmatchingchallenge.com/challenge-information/challenge-details.

31 Steven Posnack, "Demystifying Patient Matching Algorithms," *Health IT Buzz* (blog), May 1, 2017, https://www.healthit.gov/buzz-blog/interoperability/demystifying-patient-matching-algorithms/.

32 Agency for Healthcare Research and Quality, "Enhancing Patient Matching in Support of Operational Health Information Exchange (Indiana)," accessed July 24, 2018, https://healthit.ahrq.gov/ahrq-funded-projects/enhancing-patient-matching-support-operational-health-information-exchange.

33 Office of the National Coordinator for Health Information Technology, "Patient Demographic Data Quality Framework," last accessed July 24, 2018, https://www.healthit.gov/playbook/pddq-framework/; Business Wire, "CMMI Institute and the U.S. Department of Health and Human Services Launch Framework to Address Patient Data," news release, Dec. 15, 2017, https://www.businesswire.com/news/home/20171215005466/en/CMMI®-Institute-Department-Health-Human-Services-Launch.

34 ECRI Institute, "Partnership for Health IT Patient Safety Issues Recommendations for the Safe Use of Health IT for Patient Identification," news release, Feb. 20, 2017, https://www.ecri.org/press/Pages/HITPS-Issues-Recommendations-for-Patient-Identification.aspx.

35 Experian Health, "Experian Health Named 2017 MongoDB Innovation Award Winner in Healthcare Category," July 12, 2017, http://www.experian.com/blogs/healthcare/2017/07/experian-health-named-2017-mongodb-innovation-award-winner-healthcare-category/; Karly Rowe, "The Power of a Universal Identifier," *US HIT Leaders and News.com*, accessed May 15, 2018, https://us.hitleaders.news/the-power-of-a-universal-identifier-driving-healthcare-efficiency-cutting-costs-and-improving-care/; Rachel Z. Arndt, "Experian Takes on Patient ID," Modern Healthcare, Sept. 8, 2017, http://www.modernhealthcare.com/article/20170908/TRANSFORMATION02/170909929?utm_source=modernhealthcare &utm_campaign=hits&utm_medium=email&utm_content=20170908-TRANSFORMATION02-170909929*.

36 Kevin Sieff, "In Afghanistan, Jan. 1 Is Everyone's Birthday," *The Washington Post,* Dec. 31, 2013, https://www.washingtonpost.com/world/in-afghanistan-its-everyones-birthday/2013/12/31/81c18700-7224-11e3-bc6b-712d770c3715_story.html?noredirect=on&utm_term=.2454f192bb5b.

37 Social Security Administration, "Program Operations Manual System (POMS): RM 10201.010 Nonprogram Use of the Social Security Number (SSN)," updated May 26, 2017, https://secure.ssa.gov/poms.nsf/lnx/0110201010.

38 Barbara D. Bovbjerg (director of education, workforce, and income security issues at Government Accountability Office), statement before the Committee on Consumer Affairs and Protection and Committee on Governmental Operations, New York State Assembly, Sept. 15, 2005, http://www.gao.gov/new.items/d051016t.pdf; American Health Information Management Association, "Limiting the Use of the Social Security Number in Healthcare," *Journal of American Health Information Management Association* 82, no. 6 (2011): 52-56, http://library.ahima.org/doc?oid=104465#.WS7uEevyuCg.

39 Bruce Rosen and Ruth Waitzberg, "The Israeli Health Care System," accessed June 5, 2017, http://international.commonwealthfund.org/countries/israel/; John Halamka, "On the Road in China," *Life as a Healthcare CIO* (blog), Oct. 26, 2012, http://geekdoctor.blogspot.com/2012/10/on-road-in-china.html.

40 Ministry of Health New Zealand, "National Health Index," updated March 28, 2017, http://www.health.govt.nz/our-work/health-identity/national-health-index; Juliet Rumball-Smith, "Uniquely Identified: The Impact of a National Health Index," *NEJM Catalyst,* Oct. 4, 2017, https://catalyst.nejm.org/uniquely-identified-national-health-index/.

41 Dan Cidon, "How Other Countries' Struggles With Patient Identifiers Can Help the U.S.," *Health Data Management,* March 5, 2018, https://www.healthdatamanagement.com/opinion/how-other-countries-struggles-with-patient-identifiers-can-help-the-us; National Health Service, "NHS Quarterly Data Summary Issue 10: Learning From Reporting—Patient Identification," accessed July 24, 2018, http://webarchive.nationalarchives.gov.uk/20100314214240/http://www.nrls.npsa.nhs.uk/resources/type/data-reports/?entryid45=59855&cord=DESC&p=1.

42 National Health Service, "NHS Quarterly Data Summary Issue 10."

43 Government Accountability Office, "VA Information Technology: Pharmacy System Needs Additional Capabilities for Viewing, Exchanging, and Using Data to Better Serve Veterans" (2017), https://www.gao.gov/assets/690/685260.pdf; Susan D. Hosek and Susan G. Straus, "Patient Privacy, Consent, and Identity Management in Health Information Exchange: Issues for the Military Health System," RAND Corp. (2013), https://www.rand.org/content/dam/rand/pubs/research_reports/RR100/RR112/RAND_RR112.pdf.

44 U.S. House of Representatives Committee on Ways and Means, "Hearing on Removing Social Security Numbers From Medicare Cards," 112th Congress, Aug. 1, 2012, https://waysandmeans.house.gov/wp-content/uploads/2017/07/20120801SSHL.pdf; Anita Samarth, "Patient Misidentification: The Case Against the National Patient Identifier," HIT Consultant, Feb. 26, 2018, https://hitconsultant.net/2018/02/26/national-patient-identifier-case/; Karen Jackson (deputy chief operating officer, Centers for Medicare & Medicaid Services), statement before the U.S. House Committee on Ways & Means Subcommittee on Social Security and U.S. House Committee on Oversight & Government Reform Subcommittee on Information Technology, "Protecting Americans' Identities: Examining Efforts to Limit the Use of Social Security Numbers," May 23, 2017, https://waysandmeans.house.gov/wp-content/uploads/2017/05/20170523SS-Testimony-Jackson.pdf; Medicare Access and CHIP Reauthorization Act of 2015, Pub. L. No. 114-10, 114th Congress (2015), https://www.congress.gov/bill/114th-congress/house-bill/2/text.

45 Harpreet S. Sood et al., "Has the Time Come for a Unique Patient Identifier for the U.S.?" *NEJM Catalyst,* Feb. 21, 2018, https://catalyst.nejm.org/time-unique-patient-identifiers-us/.

46 Twila Brase, "Policy Insights—National Patient ID," Citizens' Council for Health Freedom (2012), http://www.cchfreedom.org/pr/Final_UPI_Report-Use(1).pdf.

47 Herox, "CHIME National Patient ID Challenge," accessed June 5, 2017, https://herox.com/PatientIDChallenge.

48 College of Healthcare Information Management Executives, "National Patient ID Challenge," accessed July 24, 2018, https://chimecentral.org/chime-npidchallenge/.

49 Centers for Medicare & Medicaid Services, "New Medicare Cards," last modified Aug. 7, 2018, https://www.cms.gov/Medicare/New-Medicare-Card/index.html; Centers for Medicare & Medicaid Services, "New Medicare Cards Offer Greater Protection to More Than 57.7 Million Americans," news release, May 30, 2017, https://www.cms.gov/Newsroom/MediaReleaseDatabase/Press-releases/2017-Press-releases-items/2017-05-30.html.

50 Christina Farr, "Would You Trust a Hospital to Scan Your Fingerprint?" KQED, Nov. 23, 2015, https://www.kqed.org/futureofyou/70484/would-you-trust-a-hospital-to-scan-your-fingerprint; Bill Siwicki, "Iris Recognition, Palm-Vein, Fingerprinting: Which Biometric Is Best for Healthcare?" *Healthcare IT News*, March 30, 2016, http://www.healthcareitnews.com/news/iris-scanning-palm-vein-fingerprinting-which-biometric-best-healthcare.

51 Joshua Engelsma et al., "Universal 3D Wearable Fingerprint Targets: Advancing Fingerprint Reader Evaluations," *IEEE Transactions on Information Forensics and Security* 13 (2018): 1564, https://arxiv.org/pdf/1705.07972.pdf.

52 Martin Drahansky, "Liveness Detection in Biometrics," in *Advanced Biometric Technologies*, ed. Girija Chetty (IntechOpen, 2011), https://www.intechopen.com/books/advanced-biometric-technologies/liveness-detection-in-biometrics; Sujan Parthasaradhi et al., "Time-Series Detection of Perspiration as a Liveness Test in Fingerprint Devices," *IEEE Transactions on Systems, Man, and Cybernetics, Part C* (Applications and Reviews) no. 3 (2005): 335-343, https://ieeexplore.ieee.org/document/1487582/; Rui Chen, Xirong Lin, and Tianhuai Ding, "Liveness Detection for Iris Recognition Using Multispectral Images," *Elsevier* 33, no. 12 (2012): 1513-1519, https://doi.org/10.1016/j.patrec.2012.04.002; Eui Chul Lee and Kang Ryoung Park, "Fake Iris Detection Based on 3D Structure of Iris Pattern," *International Journal of Imaging Systems and Technology* 20, no. 2 (2010): 162-166, https://doi.org/10.1002/ima.20227; Sheng-Hsun Hsieh et al., "A Novel Anti-Spoofing Solution for Iris Recognition Toward Cosmetic Contact Lens Attack Using Spectral ICA Analysis," *Sensors* 18, no. 3 (2018): 795; http://www.mdpi.com/1424-8220/18/3/795.

53 Kartikay Mehrotra, "Tech Companies Are Pushing Back Against Biometric Privacy Laws," *Bloomberg Businessweek,* July 19, 2017, https://www.bloomberg.com/news/articles/2017-07-20/tech-companies-are-pushing-back-against-biometric-privacy-laws.

54 Iris scans are distinct from retinal scans, which are sometimes used in national security settings but may be inappropriate in health care settings since they can be changed by disease or pregnancy.

55 U.S. Department of Commerce, "NIST: Iris Recognition Report Evaluates 'Needle in Haystack' Search Capability," *The Commerce Blog* (blog), April 23, 2012, https://2010-2014.commerce.gov/blog/2012/04/23/nist-iris-recognition-report-evaluates-needle-haystack-search-capability.html; Alan Gelb, Anit Mukherjee, and Anna Diofasi, "Iris Recognition: Better Than Fingerprints and Falling in Price," *Center for Global Development* (blog), Aug. 1, 2016, https://www.cgdev.org/blog/iris-recognition-better-fingerprints-and-falling-price; Alice Lipowicz, "NIST Tests Accuracy in Iris Recognition for Identification" *FCW*, April 23, 2012, https://fcw.com/articles/2012/04/23/nist-iris-recognition.aspx; Bayometric, "Biometric Devices: Cost, Types and Comparative Analysis," accessed March 27, 2018, https://www.bayometric.com/biometric-devices-cost/; Mehedi Hassan, "Which Is the Most Reliable Biometric Modality?" *M2SYS* (blog), Sept. 16, 2016, http://www.m2sys.com/blog/biometric-hardware/reliable-biometric-modality/.

56 National Institute of Standards and Technology, "Biometrics," updated July 13, 2017, https://www.nist.gov/programs-projects/biometrics.

57 International Biometric Group, "Biometrics Explained" (2002), http://web.science.mq.edu.au/~isvr/Documents/pdf%20files/biometrics/Biometrics%20Explained.pdf.

58 National Institute of Standards and Technology, "Minutiae Interoperability Exchange (MINEX) Overview," updated July 13, 2017, https://www.nist.gov/programs-projects/minutiae-interoperability-exchange-minex-overview; "INCITS Standardized Biometric Data," updated Dec. 14, 2016, https://www.nist.gov/itl/iad/image-group/resources/incits-standardized-biometric-data; American National Standards Institute, "ANSI INCITS 378-2004: Information Technology—Finger Minutiae Format for Data Interchange," https://webstore.ansi.org/RecordDetail.aspx?sku=ANSI+INCITS+378-2004.

59 Abhishek Nagar, Karthik Nandakumar, and Anil K. Jain, "Biometric Template Transformation: A Security Analysis," *Society of Photo-Optical Instrumentation Engineers (SPIE),* 7541, Media Forensics and Security II (2010), http://dx.doi.org/doi:10.1117/12.839976.

60 Techopedia, "Biometric Engine," accessed March 27, 2018, https://www.techopedia.com/definition/26147/biometric-engine.

61 Mishi Choudhary, "Viewpoint: The Pitfalls of India's Biometric ID Scheme," *BBC,* April 23, 2018, https://www.bbc.com/news/world-asia-india-43619944.

62 Robert S. Rudin et al., "Defining and Evaluating Patient-Empowered Approaches to Improving Record Matching," RAND Corp., accessed Aug. 27, 2018, https://www.rand.org/pubs/research_reports/RR2275.html.

63 CARIN Alliance, "About Us," accessed July 11, 2018, https://carinalliance.com/about.

64 Jingjing Jiang, "Millennials Stand Out for Their Technology Use, But Older Generations Also Embrace Digital Life," Pew Research Center, May 2, 2018, http://www.pewresearch.org/fact-tank/2018/05/02/millennials-stand-out-for-their-technology-use-but-older-generations-also-embrace-digital-life/.

65 Harmony Rhoades et al., "No Digital Divide? Technology Use Among Homeless Adults," *Journal of Social Distress and the Homeless* 26, no. 1 (2017): 73-77, https://www.tandfonline.com/doi/full/10.1080/10530789.2017.1305140.

66 Centers for Medicare & Medicaid Services, "Trump Administration Announces MyHealthEData Initiative to Put Patients at the Center of the U.S. Healthcare System," news release, March 6, 2018, https://www.cms.gov/newsroom/press-releases/trump-administration-announces-myhealthedata-initiative-put-patients-center-us-healthcare-system; Joe Biden, "Joe Biden: To Save and Improve Lives Using Data, Details Matter," *Fortune,* March 19, 2018, http://fortune.com/2018/03/19/joe-biden-cancer-moonshot-data-save-lives/.

67 Bipartisan Policy Center, "Challenges and Strategies for Accurately Matching Patients to their Health Data"; Morris et al., "Patient Identification and Matching."

68 Culbertson et al., "The Building Blocks of Interoperability."

69 Jonathan Perlin and John Halamka letter to Farzad Mostashari, Aug. 17, 2011, https://www.healthit.gov/sites/default/files/standards-certification/8_17_2011Transmittal_HITSC_Patient_Matching.pdf.

70 Culbertson et al., "The Building Blocks of Interoperability."

71 LexisNexis, "LexID: Advanced Analytics for Better Identity Management," accessed July 23, 2017, https://risk.lexisnexis.com/our-technology/lexid; National Council for Prescription Drug Programs, "Experian Health and NCPDP Align to Improve Patient Identification Across the Healthcare Ecosystem," news release, Sept. 27, 2016, http://www.ncpdp.org/NCPDP/media/pdf/pressrelease/Experian-Health-_NCPDP-Alliance-Announcement_092616.pdf.

72 Verato, "Verato Pens Letter to U.S. Senate and House Recommending Referential Matching as Nationwide Strategy," accessed May 14, 2018, https://www.verato.com/verato-pens-letter-senate-house-recommending-referential-matching-nationwide-strategy/.

73 Ibid.

74 *The Business Debate*, "Leveraging Data-Driven Technology in the Health Industry," Feb. 21, 2018, http://thebusinessdebate.com/experian-health-leveraging-data-driven-technology-in-the-health-industry/; Verato, "Verato Submits Public Comments on TEFCA Framework," Feb. 20, 2018, https://www.verato.com/verato-submits-public-comments-on-tefca-framework/.

75 Rita Torkzadeh et al., "Advancing a Nationwide Patient Matching Strategy," *Journal of the American Health Information Management Association* 89, no. 7 (2018): 30-35, http://bok.ahima.org/doc?oid=302539#.WzJlj1VKhEZ.

76 Office of the National Coordinator for Health Information Technology, "Draft Trusted Exchange Framework," Jan. 5, 2018, https://www.healthit.gov/sites/default/files/draft-trusted-exchange-framework.pdf.

77 Ben Moscovitch, "Pew Urges Better Patient Matching, Data Standards to Boost Health IT Interoperability," The Pew Charitable Trusts, Feb. 20, 2018, http://www.pewtrusts.org/en/research-and-analysis/speeches-and-testimony/2018/02/pew-urges-better-patient-matching-data-standards-to-boost-health-it-interoperability.

78 Elizabeth Snell, "Health Information Exchange Hindered by Patient Matching Issues," *EHR Intelligence*, May 11, 2018, https://ehrintelligence.com/news/health-information-exchange-hindered-by-patient-matching-issues; Accreditation Council for Pharmacy Education et al., May 9, 2018, comment letter to congressional appropriators regarding House and Senate FY19 appropriations bills, http://bok.ahima.org/PdfView?oid=302512.

79 Torkzadeh et al., "Advancing a Nationwide Patient Matching Strategy."

80 National Institute of Standards and Technology, "Digital Identity Guidelines," June 2017, https://pages.nist.gov/800-63-3/sp800-63-3.html.