Research Report

Defining and Evaluating Patient-Empowered Approaches to Improving Record Matching

Robert S. Rudin, Richard Hillestad, M. Susan Ridgely,

Nabeel Shariq Qureshi, John S. Davis II, Shira H. Fischer

For more information on this publication, visit www.rand.org/t/RR2275

Published by the RAND Corporation, Santa Monica, Calif.

Preface

The Pew Charitable Trusts, an independent nonprofit research and public policy organization, sponsored a RAND Corporation study to identify potential "patient-empowered" solutions to improve patient record matching, evaluate the solutions based on specific criteria, and, based on that assessment, select a promising solution (or cluster of solutions) within this range of approaches for further development and pilot testing. Incomplete and erroneous record matching (the process of identifying and linking medical records for the same patient across different data sources) is a widely recognized problem that impedes interoperability and health information exchange (HIE) among health care providers, increases health care costs, and hampers health care quality. Based on this study, this report documents ten potential patient-empowered solutions and 11 evaluation criteria and analyzes each solution, selecting an incremental, three-stage approach to improving record matching that combines elements of several solutions into a mobile phone solution with app-based functionality. The report concludes with recommendations for this patient-empowered approach to improve record matching. Approaches to record matching that did not involve patients were not included.

We expect this work to be of interest to all stakeholders who are directly or indirectly involved in record matching, including health care providers in the public and private sectors, patients, health information networks, health information technology vendors, and payers such as insurance companies and employers. It should also be informative to federal, state, and individual efforts to improve record matching.

This research was conducted by RAND Health, a division of the RAND Corporation, with funding from The Pew Charitable Trusts. For more about RAND Health, visit www.rand.org/health.

Table of Contents

Figures

Tables

Summary

Despite widespread adoption of electronic health records (EHRs) and increasing exchange of health care data, the benefits of interoperability and health information technology have been hampered by the inability to reliably match patients and their records. A 2014 report by the Office of the National Coordinator for Health Information Technology (ONC) suggested that when providers exchange records with other providers, rates of record matching—defined as the process of identifying and linking medical records for the same patient across different data sources—can be as low as 50 percent. Other studies suggest that even with dedicated effort, these rates may not reach above 95 percent. Because of inadequate record matching, too often, some or all of a patient's medical data are not made available at the point of care or, more worrisome, incorrect patient data are used to make medical decisions. It is widely recognized that correct record matching is critical to prevent medical errors, avoid delays in care, facilitate informed medical decisionmaking, and reduce administrative burdens.

The Pew Charitable Trusts contracted with the RAND Corporation to investigate "patient-empowered" approaches to record matching—solutions that have some additional, voluntary role for patients beyond simply supplying demographics to their health care providers—and to select a promising solution for further development and pilot testing. (Other types of record matching solutions in which the patient does not have an added role exist and are the subject of other studies supported by Pew and conducted by other investigators. We did not compare patient-empowered approaches to other approaches.) This work occurred in two phases. In Phase 1, we identified possible solutions and criteria to evaluate them through literature searches, as well as interviews with subject matter experts (SMEs) and an expert panel, who provided feedback and helped us select a solution. In Phase 2, we further specified the selected solution and next steps by conducting additional interviews, targeted literature searches, and by meeting with the expert panel a second time.

While we did not identify a "silver bullet" solution, we did identify multiple patient-empowered approaches that may have potential—with further development—to improve record matching. Ultimately, we selected *a three-stage solution in which patients can "verify" their mobile phone number and other identity attributes with their health care providers and use new smartphone app functionalities that enable bidirectional communication of identity and health information between patients and providers.* We make recommendations for how to advance this solution through development and pilot tests.

Evaluation Criteria for Record Matching Solutions

Through analysis of literature and with expert input, we identified 11 evaluation criteria for making systematic comparisons of record matching solutions (criteria are neither independent of one another nor mutually exclusive):

1. Improvement in record matching if widely implemented
2. Patient control
3. Likelihood of adoption by patients
4. Likelihood of adoption by providers
5. Likelihood of adoption by vendors
6. Feasibility (of development, pilot testing, and implementation)
7. Minimal security risks
8. Sustainability (operational and financial)
9. Political viability
10. Potential to foster new uses of matched records
11. Low potential for unintended negative consequences

The large number of criteria reflects the complexity of the record matching design space and the potential need for nuanced tradeoffs. This complexity is also apparent in the ongoing challenges with record matching, the diverse potential solutions we identified, and the lack of clear consensus among experts on a favored solution.

Patient-Empowered Solutions to Record Matching

Through analysis of literature and with expert input, our study identified ten potential solutions that involve additional patient participation. Solutions involved a range of new patient activities, including supplying new or enhanced patient identity information to health care providers (which can be used in record matching processes); giving health care providers record location information or access to their aggregated medical records; and participating in verifying information to improve record matching. The ten potential patient-empowered solutions are:

1. Implementing a voluntary universal identifier (VUID): A central organization issues identifiers but does not store protected health information (PHI); providers manage identifiers using hardware and software that is supplied by the central organization and interfaces with their existing systems.
2. Using a public key as an identifier: Patients are issued a public key–private key pair and use the public key as identifier.
3. Expanding the use of existing government-issued identifiers: Patients provide driver's license or other IDs, which are used with demographics for record matching.
4. Adding knowledge-based identity information: Patients answer knowledge-based questions, which are used with demographics for record matching.
5. Adding biometric data: Patients provide fingerprints, iris scans, or other biometrics, which are used along with demographics for record matching (multiple technical architectures are possible).

6. Having patients verify identity information: Patients verify existing identity information such as mobile phone number through one-time passcodes sent by their provider.
7. Using consumer-directed exchange: Patients collect their health information into one application and can access and share it with providers.
8. Using health record banks (HRBs): Providers submit health records to a regional data repository that allows patient and provider access.
9. Having patients manually verify record matches: Patients verify record matches or identify lack of matches through a user interface.
10. Having patients supply record location information: Patients provide information on previous care locations that providers use to identify previous records.

While we were able to find extensive information regarding some of the proposed solutions, the available information for others consisted of overarching ideas or concepts that had not been fully developed. Solutions also ranged widely in important aspects such as type of data to be used for record matching, degree of patient involvement, and workflow changes that would be required of health care providers.

Evaluation of Identified Solutions

We encountered a number of challenges in applying the evaluation criteria and selecting a promising approach for further development and pilot testing. Some proposed solutions were based on general ideas and lacked important functional detail needed to define how they worked. Others were fully developed and had been pilot tested, but formal evaluation data were unavailable and/or the generalizability of evaluation results was questionable. Nevertheless, we were able to systematically apply our 11 evaluation criteria to our ten potential solutions and compare the relative strengths and limitations of the various solutions. No solution emerged as the "silver bullet," and some challenges were common across many solutions. We ultimately selected an approach that combines aspects of several of the solutions.

Our analysis found two core challenges to patient-empowered record matching solutions: (1) patients, in general, are unaware of record matching issues, or may believe that the health care system should fix the matching problem without their involvement, and (2) providers may be reluctant to make major changes in staff workflows, core business and administrative processes, and technology, even for the limited time required to pilot a solution. These challenges notwithstanding, we found that the appeal of some of the solutions is obvious, and yet their drawbacks are also evident. For example, biometrics-based approaches are surely convenient, but at the same time, fingerprints cannot be changed if they are compromised. Consumer-mediated exchange solutions (which we define to include HRBs and consumer-directed exchange) are ideal for promoting patient control, but they have questionable return on investment and thus may lack the business rationale necessary for widespread adoption. On balance, a reasonable argument could be made to further develop and pilot test most of the

potential solutions we identified, and in fact, for many of the potential solutions, some experts claimed the benefits would exceed the costs.

As a result of our analysis, and in consultation with Pew staff and our expert panel, we selected for further development an approach to patient-empowered record matching that combines and enhances several of the potential record matching solutions we identified. In particular, we propose to involve patients in verifying their identity information (Solution 6); using smartphone apps to share government-issued identifiers with providers (Solution 3); using smartphone app credentials to log in to their patient portals, which may ultimately facilitate consumer-mediated exchange (Solution 7); and using smartphone apps to store and use an identifier similar to the one proposed as part of the HRB model (Solution 8). This approach involves developing multiple complementary functionalities that work together in a synergistic way and can be implemented in a stepwise fashion, with each successive stage offering incrementally greater potential for improving record matching. All of the proposed components are centered on the functionality afforded by mobile phones and smartphone apps. We chose this approach because it could:

- leverage the widespread and increasing adoption of mobile phones and smartphones;
- improve record matching because of improved data quality of identity information and use of attributes that have been verified;
- leverage and integrate with providers' and health information networks' (HINs') existing record matching engines;
- promote the use of a simplified check-in process at providers' front desks (thereby improving the likelihood of adoption by patients and providers); and
- evolve to incorporate additional functionality to improve record matching and increase patient access to and control over their data.

However, we acknowledge that this approach also has some disadvantages, including the need to establish new technical specifications and new provider workflows, as well as the potential to exclude some patients (such as those who cannot afford smartphones or have difficulty using them) from benefiting from some components. While development and pilot work on this solution are feasible with modest resources, scaling the solution (or any patient-empowered record matching approach) may require an extensive effort of national scope.

Three-Stage Solution

Our solution takes a phased approach by starting with components that we anticipate would be easier to put in place. This solution aims to improve the quality of identity information used for record matching (Stage 1), establish new functionalities of smartphone apps (which may consist of apps that currently exist, such as those that currently support personal health records [PHRs], or newly developed apps) to facilitate transfer of this information to providers (Stage 2), and create advanced app functionality to further improve record matching and address our other evaluation criteria (e.g., likelihood of adoption, sustainability) (Stage 3). We describe this

approach in terms of three stages that we believe are the most likely sequence for development and implementation, but it is possible that some components may be developed or implemented earlier or later than we describe relative to others (e.g., smartphone app functionalities for transferring identity information to providers may be developed before the concept of verified identifiers is established and implemented). See Table S.1 for a summary of the key components.

Table S.1. Three-Stage Solution to Patient Record Matching

Stage 1: Add Verified Patient Identity Information	Stage 2: Add Basic App Functionality	Stage 3: Add Advanced App Functionality
• Technical specifications for verified attributes are established • Workflows and best practices to verify attributes starting with mobile phone numbers are developed • Workflows and best practices to facilitate patient sign-up for existing patient portals are developed	• Technical specifications define APIs that enable bidirectional communication between a patient app and provider • Patient app can send identity information (including attributes verified by app) • App can return provider contact info and instructions to sign up for patient portal • Governance ensures apps are trusted	• Apps can facilitate identity-proofing to increase number of verified fields • Credentials from app can be used to log in to patient portals, facilitating health data aggregation in app • Validated insurance information can be stored in app and transferred to provider with other identity attributes • Unique identifiers issued by HINs can be stored in app and transferred to provider with other identity attributes

The first stage introduces the concept of "verified" patient identity attributes, which would mean that the attribute had been confirmed by the patient. Such an attribute would be used by record matching engines along with existing attributes and would be weighted as more reliable because it was verified. This enhancement to identity information will improve the accuracy of record matching engines and would enable immediate use of verified mobile phone numbers, which are existing identifiers that have many good qualities for improving (but not perfecting) record matching: They are unique, they change infrequently, they are controlled by an existing international infrastructure, and patients have a strong incentive to avoid having their phone stolen or phone number compromised. This concept of verified attributes will require the development of technical specifications for verified data fields that assign a level of data quality to patient identity information.

The second stage provides basic functionality of a smartphone app that would transfer identity information (e.g., name, date of birth, address, government-issued identifiers) to health care providers, replacing paper clipboards for this information, and, in turn, facilitating the transfer of patient health data from patient portals into the app. Although each patient will likely use only a single smartphone app, in an ideal world we envision patients having multiple options from which to choose. In the third stage, advanced app functionalities would be developed to improve record matching and strengthen the value proposition for both patients and providers.

Examples of such functionality include using an app to identity-proof patients, expanding existing efforts by HINs to issue unique identifiers to patients, which they can use through their smartphone apps, and allowing patients to log in to their patient portals using their smartphone app credentials. This work will require iterative testing to develop the functional requirements and specifications so that such apps are usable and useful, and may require a governance process to ensure apps are trusted by patients and providers.

Recommendations

We provide five recommendations, three of which advance our selected three-stage solution through development and pilot testing and two that would help to accelerate any and all efforts to improve record matching. For the first three recommendations, to support development, pilot testing, and evaluation of the components of the three-stage solution, a source of funding would be required to pay application designers, software developers, evaluators, and possibly other participants. To achieve widespread adoption, the technical specifications and best practices resulting from the development efforts we recommend would need to be widely and freely available, and so funding for them would most likely need to come from stakeholders dedicated to improving record matching broadly rather than those who expect to make a profit.

Recommendation 1. Develop technical specifications for verified data fields, develop best practices that allow health care providers to verify mobile phone numbers, and iteratively pilot test and refine the specifications and best practices to maximize feasibility and usability. In Stage 1 of our solution, the concept of a verified data field, especially applied to mobile phone numbers, can improve record matching rates by providing higher quality data for matching engines and metadata indicating the degree of quality (e.g., metadata that indicated a phone number was verified last week would suggest the phone number was more reliable than if it was verified five years ago or not at all). The technical specifications and best practices should be developed by a team of application designers and software developers and pilot tested with at least two participating provider organizations that share patients and use a matching engine. As feasibility is demonstrated, pilot testing with new types of providers in different settings and with patients would allow for further refinement and scaling up.

Recommendation 2. Develop application programming interfaces (APIs) and best practices for establishing bidirectional communication between a smartphone app and health care provider registration systems at the point of care, and iteratively pilot test and refine them. In Stage 2, development should assess the use of quick response (QR) codes or near-field communication (NFC) to allow a smartphone app to transfer identity information to health care providers and facilitate patient access to their health information through their patient portal accounts. As with Stage 1, this development work should be done by application designers

and software developers and pilot tested with at least two participating provider organizations that share patients and use a matching engine. One or more smartphone app vendors would also need to participate. As feasibility is demonstrated, additional pilot testing with new types of providers in different settings and with patients will help further refinement. To facilitate widespread adoption, the API should not be proprietary.

Recommendation 3. Develop advanced app functionalities. In Stage 3, advanced smartphone app functionalities may include one or more of the following: establishing mechanisms to remotely identity-proof a patient from a smartphone app, allowing credentials that are associated with control of the phone to be used to log in to a patient portal, incorporating verified insurance information in an app, and using identifiers from "qualified" HINs (as defined under the Office of the National Coordinator's Trusted Exchange Framework and Common Agreement [TEFCA]). Other advanced app functionalities should also be considered to improve the value proposition for patients and providers. This work would be undertaken by application designers and software developers, but, depending on which functionalities are chosen and the development work required, other stakeholders (e.g., identity-proofing services, insurance companies, HINs) would have to be involved as well.

Recommendation 4. Establish or designate an organization to oversee national progress in record matching. An organization is needed to provide leadership, convene stakeholders, monitor and track progress, spread best practices, potentially help establish governance processes, and try to keep record matching on the agenda as a high priority for the public and for health system leaders. This organization could be a new or existing organization, and it could be public or private, but it should be recognized in some capacity by the federal government so as to provide legitimacy and promote transparency. The organization could be established by making a long-term commitment to this issue and convening key stakeholders or by being designated by the federal government. Its specific role should evolve over time according to the needs of ongoing record matching efforts and should not duplicate other organizations' capabilities (e.g., standards development).

Recommendation 5. Conduct more rigorous research into the nature and magnitude of record matching errors, and create methods for health care providers to objectively benchmark their record matching performance. Despite recognition of the importance of record matching, few studies have investigated its causes or measured matching rates, and health care providers do not report matching rates publicly. As a result, few patients are aware of the problem, which may, in turn, be depressing demand for a solution. Objective analyses of the financial and clinical burdens of record matching failures will increase the urgency of addressing this problem. More research into the causes of record matching error, development of methods for health care providers to benchmark their matching rates, and requirements to publicly report

matching rates would help provide much-needed transparency and make the case for scaling solutions.

Conclusions

In this study, we identified a range of potential solutions to engage patients in record matching in a way that could address current matching failures, thereby strengthening interoperability and health information exchange (HIE). Although we have selected a three-stage solution and provide recommendations to further its development, this selection is not meant to discourage the development of other solutions we identified or those we did not discuss because they were outside the scope of this project. Indeed, we did not identify a patient-empowered "silver bullet" solution that would completely satisfy all of our identified evaluation criteria and produce perfect record matching—such a solution probably does not exist. Instead, engaging patients in solving the problem of inadequate record matching likely requires an array of solutions, each of which will address the problem to varying extents depending on the patient population, provider type, and care setting, as well as on provider workflow and other factors that will be identified only with real-world pilot testing and evaluation. Given high uncertainty as to the extent to which any specific solution can ultimately succeed in improving record matching, further investigation, development, and pilot testing of a range of solutions are warranted.

Acknowledgments

We would like to thank our technical expert panel (TEP) members, subject matter experts (SMEs), and quality assurance reviewers (John Halamka and Carter Price) for their time, valuable insights, and feedback on this report. In particular, we would like to thank Josh Mandel and Barry Hieb for providing comments and guidance through many formal and informal conversations, and especially David McCallie for his multiple rounds of feedback and sharing his expertise, experience, ideas, and critiques.

Please note that all SME and TEP-member comments represent their own personal views. Nothing in this report should be taken as an official statement or endorsement from the federal government or any other expert-affiliated organization.

Abbreviations

API	Application Programming Interface
ASTM	American Society for Testing Materials
CCDA	Consolidated Clinical Document Architecture
CHIME	College of Health Care Information Management Executives
CMS	Centers for Medicare and Medicaid Services
ED	emergency department
EHR	electronic health record
FHIR	Fast Health Interoperability Resources
FIDO	Fast IDentity Online
FTC	Federal Trade Commission
GPII	Global Patient Identifiers, Inc.
HHS	U.S. Department of Health and Human Services
HIE	health information exchange
HIN	health information network
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health
HRB	health record bank
IAL	identity assurance level
MiHIN	Michigan Health Information Network Shared Services
MPI	master patient index
NFC	near-field communication
NIST	National Institute of Standards and Technology
ONC	Office of the National Coordinator for Health Information Technology
PHI	protected health information
PHR	personal health record
QHIN	qualified health information network
QPP	Quality Payment Program

QR	quick response
RCE	recognized coordinating entity
SME	subject matter expert
TEFCA	Trusted Exchange Framework and Common Agreement
TEP	technical expert panel
U2F	universal 2-factor
UHID	unique health identifier
UPI	universal patient identifier
VUID	voluntary universal patient identifier
WEDI	Workgroup for Electronic Data Interchange

1. Introduction

As the use of electronic health records (EHRs) becomes more widespread and health care data is increasingly exchanged among provider organizations, the inability to reliably match patients with their medical records has become a persistent scourge, as well as a bottleneck to reaping the benefits of interoperability and *health information exchange* (HIE).[1] Patient *record matching* is the process of identifying and linking medical records for the same patient across different data sources—whether this is being done internally by a provider or through HIE among different providers. The focus of this report is the latter. Too often, some or all of a patient's medical data are not made available at the point of care. More worrisome, incorrect patient data may be used to make medical decisions. These problems are due to record matching failures. It is widely recognized that correct record matching is critical to preventing medical errors, avoiding delays in care, facilitating informed medical decisionmaking, and reducing administrative burdens (Morris et al., 2014; Office of the National Coordinator for Health Information Technology [ONC], 2015). If a patient's records cannot be effectively matched across health care provider organizations, the full promise of federal and state investments in interoperability and HIEs will not be achieved (Hillestad, Bigelow, Bower, et al., 2005; Walker et al., 2005).

Currently, patient record matching among providers generally occurs when front desk staff use patient demographic data (e.g., name, date of birth, address) to manually locate the patient's record or when *matching engines* use algorithms to link records. For example, when a provider sends a query to look for external records through an HIE or other data network, the query includes these demographic data elements, which are then compared through matching algorithms to identify candidate record matches. Those determined by the algorithm to have a high probability of matching may be returned to the provider. However, the algorithms may fail to find the patient's records or, less often, identify the wrong patient's records. These problems occur because different patients may have similar or identical demographic information (e.g., thousands of patients in Texas are named "Maria Garcia," hundreds of whom also have the same date of birth) (Bipartisan Policy Center, 2012), or because patients change aspects of this information, such as when they change names (due to a life event) or change addresses (due to a move). Front desk staff may also make clerical errors when entering a patient's demographic information, resulting in inaccuracies or duplicate records.

[1] Words or phrases that are italicized in the document are defined in the Glossary of Terms (Appendix A).

There are many possible approaches to improve record matching. In this report, we examine a subset of approaches that involve a new role for the patient; we call this class of approaches *patient-empowered* record matching. Patients, one may argue, are an underutilized resource for improving matching of their records. After all, patients usually know who they are, often have at least some knowledge of what kinds of information should or should not be in their medical records (e.g., a nondiabetic should not have discussion of diabetes treatment), and have the most at stake if records are not matched accurately. Furthermore, solutions involving patients themselves may provide an opportunity to honor patient preferences for sharing their data. There is a range of options and tradeoffs among such solutions. The devil is in the details: The success of any solution will depend on the specific functionality of the solution itself and the context in which it is implemented.

Objectives and Scope

The Pew Charitable Trusts contracted with the RAND Corporation to investigate patient-empowered approaches to record matching, which are a subset of a larger set of possible approaches to record matching. Our objectives were to:

- identify and describe a wide range of patient-empowered approaches to record matching;
- evaluate the approaches and select a promising one among them; and
- outline next steps to advance our selected approach, including further development, pilot testing, and evaluation.

In addressing the project objectives, and to avoid duplication with other contemporaneous record matching work being supported by Pew, we first sought specific record matching solutions that had some additional, voluntary role for patients beyond the current method of supplying demographics. We anticipated that solutions would vary in terms of the degree to which patients would be engaged. For example, some solutions would allow for patients to have granular control of record matching, based on data type, visit type, or clinician role; others would offer a much more constrained role such as opt-in or opt-out. Because of this focus on a new patient role, we excluded efforts to improve algorithms used by matching engines and attempts to standardize existing identity fields.

Second, we excluded from our analysis a government-issued birth-to-death universal patient identifier (UPI). RAND researchers evaluated the costs, benefits, political issues, and privacy implications of this approach in prior work (Hillestad, Bigelow, Chaudry, et al., 2008). We did, however, include an implementation of a voluntary UPI solution that could be managed by government or a private organization.

Third, we focused on solutions to record matching for purposes of health care delivery and did not include methods of matching records for purposes of research, public health reporting, or any other secondary goals. We expect that some of the solutions we identified may also help with those activities, as well.

Finally, we focused primarily on solutions to record matching for data exchange *between* organizations. Although solutions that reduce duplicate records *within* provider organizations (e.g., use of local biometric readers at check-in) may also reduce matching errors between organizations, such as by eliminating duplicates, we were primarily interested in solutions that would address the anticipated increase in record matching failures that will emerge as interoperability and inter-organizational data exchange increases.

Organization of the Report

To investigate patient-empowered approaches to record matching, we identified as many potential solutions as we could find, identified criteria needed to evaluate these solutions, compared their relative strengths and limitations, and ultimately selected a three-stage approach. In Chapter Two, we provide background on record matching, including processes and methods for matching records under various data exchange types, and we identify key drivers of record matching errors. Chapter Three describes our research methods, which included the use of literature review, expert informant interviews, and a technical expert panel (TEP), as well as study limitations. Chapter Four describes the 11 evaluation criteria we identified for assessing and comparing the record matching solutions. Chapter Five describes the potential solutions we identified, and then applies the evaluation criteria to the identified solutions. In Chapter Six, we describe the three-stage solution we selected, and in Chapter Seven we apply the evaluation criteria to that solution. Finally, Chapter Eight summarizes our findings and offers recommendations for next steps.

2. Background

Record Matching and Health Information Exchange

Following federal investments in health information technology under the Health Information Technology for Economic and Clinical Health Act (HITECH Act), providers have increasingly adopted EHRs, but HIE between providers has lagged (HITECH, 2009; ONC, 2016). Challenges with record matching have been identified as a critical barrier to HIE (Morris et al., 2014; ONC, 2015). Methods of record matching vary by type of data exchange. The ONC defines three types of data exchange:

- *Directed exchange* (sometimes called "push") occurs when one provider sends a secure message to another provider. For example, a patient's primary care physician may send a message about a patient to a specialist who is also treating that patient (ONC, 2018c).
- *Query-based exchange* (sometimes called "pull") occurs when a provider requests information from other providers about a specific patient. For example, an emergency room physician may query other providers directly or through a regional or national *health information network* (HIN) in an attempt to gather as much information as possible about a recently admitted patient (ONC, 2018c).
- *Consumer-mediated exchange* occurs when a patient controls his or her own data and sends it to chosen providers.

In directed exchange, as defined above, record matching is typically done by a matching engine that uses a combination of deterministic and probabilistic matching algorithms to compare the message's identity information (typically demographic data elements, such as name, date of birth, and address) to the corresponding data elements of existing records in the EHR. The matching engine determines whether two records belong to the same patient by assessing whether the probability of a match falls above or below specified thresholds. If that probability is above a certain threshold, the message will be linked to the record. If the probability is below a lower threshold, the message will be considered as that of a new patient. If the probability is between those thresholds, the message may be made available for manual adjudication. (For providers who do not have access to a matching engine, all incoming records are matched manually.)

In query-based exchange, a matching engine is used by HINs rather than providers.[1] HINs use their matching engines to compare the identity information of records available from any provider in their network. As with directed exchange, if the probability of a match is above a

[1] In the case of a provider querying another provider outside of a HIN, the EHR software would perform the matching.

certain threshold determined by the HIN, the records will be linked. (Some HINs store these links so that future queries still return the same records even if identity information, such as the patient's address, has changed.) If the probability is below a different threshold, the records will be considered to belong to two separate individuals. If the probability is between those thresholds, the records may be made available for manual adjudication. With this type of data exchange, an emergency department (ED) physician would send a query to an HIN to obtain the health records of a patient, and only records that are matched to that patient's identity information by the HIN's matching engine would be returned.

Consumer-mediated exchange has its roots in the idea of a personally controlled health record, currently referred to by the term *personal health record* (PHR). A PHR is intended to be an aggregation of all of a patient's health data from multiple health care providers in one digital location. Once adopted, this type of data exchange has the potential to replace the other forms of exchange because patients would maintain one aggregate record as the "source of truth" and share it directly with their providers when they seek treatment. For example, if a patient shares her entire record with her provider, the provider would not need to query other providers for it. Likewise, if a provider sends a message to another provider, the message could be sent "through" the patient's PHR. New data generated by providers would then be added to the PHR after each visit. (Legacy data in provider's EHRs would also need to be added to the PHR.) This would, in theory, solve inter-organizational record matching issues (for those patients and providers who use it) by avoiding the need for matching engines that use patient identity attributes (Cimino et al., 2014). However, providers would still need to make sure that they identify the correct patient at the point of care and link the patient-controlled data with the correct record in their local EHR. The concept of a digital PHR was first described in 1994 by Peter Szolovits and colleagues at the Massachusetts Institute of Technology in the *Guardian Angel* manifesto (Szolovits et al., 1994). Since then, many attempts have been made to implement this vision in the context of research projects, private companies, and national efforts (Grunwell et al., 2015). However, we are unaware of a widely adopted implementation of this type of data exchange in which providers accept data from a patient's PHR, and it may never completely replace query-based or directed exchange.

These three types of HIE are not mutually exclusive and can be used within the course of a single workflow or patient encounter. For example, when a patient comes in for a routine office visit, her provider might initiate a query via the EHR to retrieve her medical records from other providers (query-based exchange), and then send a referral to another provider (directed exchange).

Record Matching Errors

Record matching is a persistent problem for provider organizations and HIEs (Bipartisan Policy Center, 2012). A 2014 survey by the College of Health Care Information Management

Executives (CHIME) reported that almost one in five chief information officers (CIOs) attributed an adverse event to patient-matching issues within the last year (CHIME, 2012). Although accuracy of matching rates is not widely reported (as there is no requirement to do so), an analysis done by the Sequoia Project (2015) suggests that, when providers exchange records with each other, matching rates may be as low as 10 to 30 percent. With considerable effort in data cleaning and algorithmic refinement among data exchange partners, it is possible to improve record matching to approximately 95 percent.

Record matching methods that rely on algorithms using demographic information may result in false negatives or false positives because patients often have similar or identical names, genders, and even dates of birth, and some data elements change over time, such as addresses. See Table 2.1 for examples of record matching errors for different types of data exchange. Although algorithms have improved over time, and there are ongoing efforts to refine them, record matching errors continue to occur. Matching processes that rely on clinicians or other staff for manual validation may also be prone to human error, as well as delays. As provider network sizes increase, the pool of similar identity information also increases, and thus, so do the challenges to finding the correct patient.

Table 2.1. Types of Inter-Provider Record Matching Errors and Examples

	False Negative (Failure to Match)	False Positive (Merged or Linked Records of Different Patients)
Directed exchange	Record received via *DIRECT message* or other notification is not linked with/merged into patient's record to whom it belongs and is added as a new patient record	Data received via a *DIRECT message* or other notification gets linked with/merged into the incorrect record
Query-based exchange	Query of data in a community HIE fails to discover patient's record Query of a vendor-based HIE returns many patient records that could be a match, but the correct one is not identified because of the manual effort required	Queried data locates incorrect patient's record and gets linked with/merged into local record
Consumer-mediated exchange	A patient shares her medical data with her provider, who mistakenly thinks it belongs to a new patient and so creates a new record	A patient shares her medical data with her provider, who then merges it into a different patient's record

Matching errors often stem from data quality issues. Clerical errors, which may be due to typos or challenges reading patient handwriting, include incorrect ordering of first, last, or middle names; other name-related errors; mistyped Social Security numbers; or simply the lack of entering demographic information (Just et al., 2016). Married couples often have the same

Social Security number listed in their records because that number is typically used for billing purposes, and health insurance is usually in the name of one spouse. As previously mentioned, sometimes existing records are not found because of name or address changes. People who are homeless present particular challenges for record matching because front desk staff use a variety of proxy addresses, such as hospitals, shelters, or places of worship, and there is no standard field to indicate homelessness (Zech et al., 2015).

These errors may also produce duplicates or incorrectly merged records within an organization, which can be propagated, causing further complications at other institutions. For example, when a scheduler calls a patient about an ordered laboratory or imaging test, the scheduler is often required to manually look up the patient in a separate system, and if the patient's record cannot be found quickly, the scheduler might create a new record (a duplicate) or accidently use the chart of a patient with similar demographics (Alreja et al., 2011; Ponemon Institute 2016). The extent of matching issues varies widely because of differences in workflows, EHR vendors, and scheduling systems.

Providers may encounter challenges when trying to improve record matching through better registration and scheduling processes. Challenges include time pressure, registration staff turnover, lack of training resources, and lack of executive support (Dooling et al., 2016). Organizations may need assurance of a return on investment to prioritize record matching, and such a return may be increasingly likely under accountable care models. However, today even highly motivated leaders of provider organizations have limited ability to improve record matching when exchanging data with other providers without enormous effort and coordination with their data exchange partners (The Sequoia Project, 2015).

Policy Context

Federal policy has shaped record matching directly and by its influence on the landscape of HIE and patient access to and control of their health data, and it may have future effects on the incentives for providers to participate in efforts to improve data exchange and record matching (Mello et al., 2018). We discuss several laws and regulations as background context.

Patient record matching challenges were recognized by policymakers as a key barrier to effective data exchange long before EHRs were widely adopted. In 1996, the Health Insurance Portability and Accountability Act (HIPAA) was passed by Congress and signed into law. It created the concept of a "covered entity," which includes health care providers and insurance plans. With some exceptions, covered entities are allowed under HIPAA to exchange data for purposes of treatment, payment, and operations, without requiring explicit patient consent. HIPAA also mandated the creation of a UPI to improve patient identification and record matching among covered entities. However, after concerns were raised by privacy advocates and others, Congress forbade the Department of Health and Human Services (HHS) from promulgating a UPI or expending any resources to develop it, forestalling federal efforts

(Paul, 1998; Greenberg and Ridgely, 2008). Patients are allowed under the HIPAA Privacy Rule to have access to their own health records for a reasonable fee, which provides some access but no technical capabilities for consumer-mediated exchange (Office of Civil Rights, 2016).

The 2009 HITECH Act provided $30 billion in direct incentives to promote "meaningful use" of different kinds of health information technology (IT) functionalities (HITECH, 2009). This effort was led by the ONC and Center for Medicare and Medicaid Services (CMS), and later became part of the Quality Payment Program (QPP) under the Medicare Access and CHIP Reauthorization Act (MACRA, 2015). Under this law, certification criteria were established for EHR products that support specific functionalities and capabilities. Eligible hospitals and providers who used certified EHRs, and met specific criteria for using them, received the incentive payments. Since the passage of the HITECH Act, adoption of EHRs has grown considerably (Henry et al., 2016). HIE has also increased but not as quickly as expected (likely due in part to persistent record matching challenges) (Greenberg and Ridgely, 2008; Greenberg, Ridgely, and Hillestad, 2009; Blumenthal, 2018). Meaningful use requirements and incentives spurred the adoption of patient portals that allow patients to log in and access their data that reside within a specific provider's EHR; these portals provide infrastructure to help enable consumers to obtain access to their records electronically (and without charge). The provision of APIs that enable download of the data has created new opportunities for consumer-mediated exchange (ONC, 2016; "Blue Button," 2017).

Possibly in anticipation of greater patient access to their records, and the future ability to participate in consumer-mediated exchange, the HITECH Act also instructed the Federal Trade Commission (FTC) to issue a Health Breach Notification Rule that encompasses "vendors of personal health records" and "PHR related entities." (A PHR is defined as an electronic record of "identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual" [42 CFR 318].) This new rule provides instructions for how PHR vendors and PHR-related entities must respond when a breach occurs (FTC, 2010).

Three provisions of the 21st Century Cures Act of 2016 are relevant to record matching. First, the Cures Act required EHR vendors as a condition of certification to support *Application Programming Interfaces* (APIs) so that patients and third-party applications can access and exchange health data "without special effort" (21st Century Cures Act, 2016). Second, the Cures Act required the ONC to create a *Trusted Exchange Framework and Common Agreement* (TEFCA) that would establish a common set of rules governing HIE, which would enable national-scale network-to-network interchange of health data (ONC, 2018a, 2018b). The ONC released for public comment a draft of TEFCA that proposes principles for data exchange, a "recognized coordination entity," and minimum required terms and conditions for data exchange (ONC, 2018a, 2018b). It also includes a proposed common set of standard demographic data elements that could be used for record matching and principles surrounding individual access to their records. Third, the Cures Act directed the ONC to issue a rule to address "information

blocking" processes (defined as process that are "likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information"), which is expected to be issued in 2018 (21st Century Cures Act, 2016). It is unknown if or how the ultimate rule will affect HIE or record matching.

Finally, ongoing policy efforts to promote value-based payments may ultimately change the incentives faced by health care providers, such the Medicare Shared Savings Program (established by the Affordable Care Act in 2011), by holding them accountable for the cost and quality issues that arise as a result of the lack of HIE and failure to match records (Patient Protection and Affordable Care Act [PPACA], 2010).

3. Methods

Our research took place in two phases. To identify potential solutions and evaluation criteria in the first phase, we first conducted a literature search, interviewed 12 subject matter experts (SMEs), and hosted a TEP (see Appendix B). Then, based on those findings, we selected a three-stage solution for further investigation. For the second phase, we conducted an additional 20 SME interviews, conducted a targeted literature review, and hosted a second TEP meeting. We iteratively refined the technical requirements, identified governance issues, and formulated recommendations for further development and pilot testing. We describe each step of our approach below. In the remaining chapters we refer to experts, which may include SMEs or TEP members.

Phase 1: Identifying Potential Solutions and Evaluation Criteria

Literature Search Methods

Data Sources and Searches

We conducted a literature search of the PubMed, Association for Computing Machinery (ACM) Digital Library, Institute of Electrical and Electronics Engineers (IEEE) Xplore Digital Library, and Web of Science databases from January 1, 2007, to July 21, 2017, to identify English language articles that reported on different patient record matching solutions. We also searched the grey literature (nonacademic sources) for government reports and other publications related to patient record matching. We used several combinations of search terms to identify these articles, such as "patient matching" and "record matching" (see Appendix C for a complete list of terms). We added additional articles suggested by members and colleagues of the research team and by experts we interviewed (see below).

Study Selection

Inclusion criteria: We included publications describing design choices and contextual factors relevant to a patient record matching solution. Design choices included decisions or assumptions that were made to implement a specific solution to patient matching. Contextual factors included any circumstances that could affect the implementation or effectiveness of a matching solution, including characteristics of the country of origin, method of implementation, and stakeholder reactions. Publications that did not include design decisions or contextual factors were excluded.

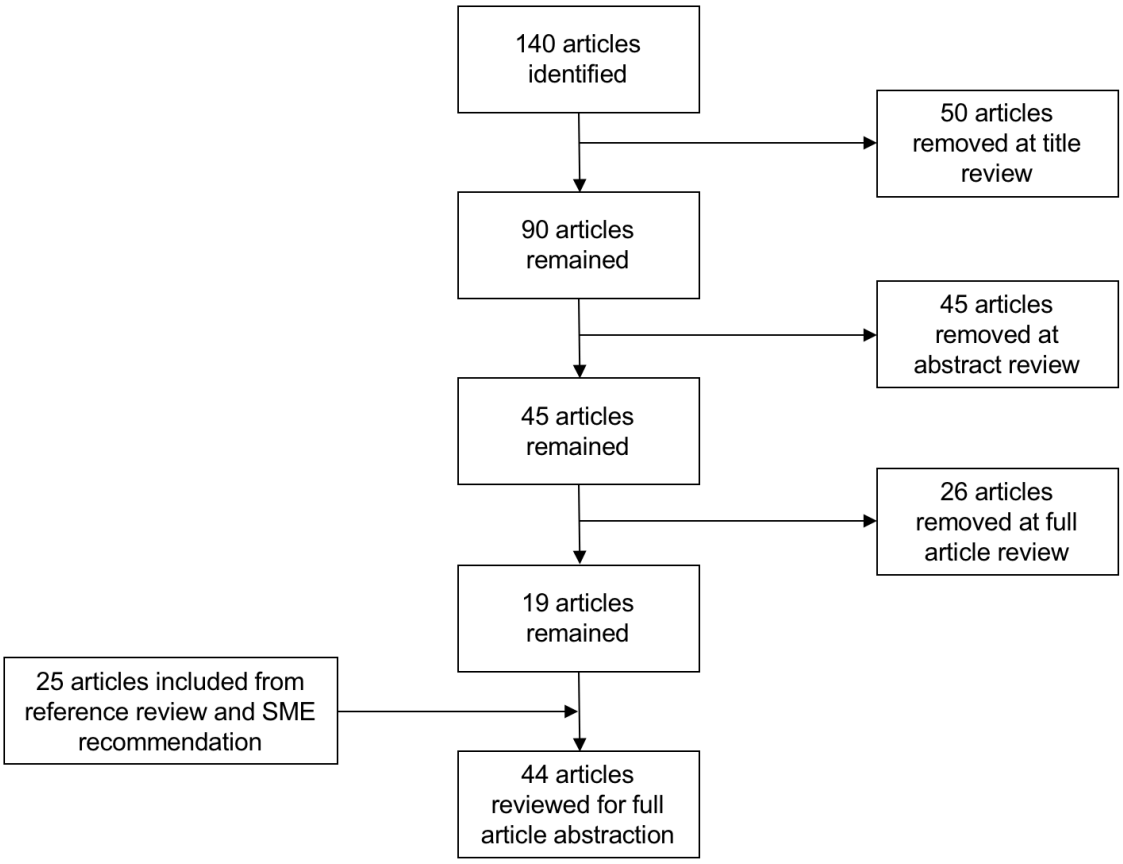
Selection process: Articles were screened in three rounds based on title (for publications that were clearly about unrelated topics), abstract, and full text. For each round, one of two research team members (RSR and NQ) conducted an initial screening, and the other reviewer either

confirmed the decision or suggested a different screening outcome. All disagreements were resolved by consensus among the two reviewers.

Data Extraction and Quality

Articles included after full-text screening were abstracted by one researcher and verified by another to confirm inclusion and capture of all relevant information. For each article, we extracted the publication year, a brief summary of the article's contents, the contextual factors presented, and the design choices mentioned.

Figure 3.1. Literature Flow



Expert Engagement

To ensure we captured the latest thinking and developments, we sought extensive expertise from SMEs and others through a TEP, as described below.

Key Informant Interviews

We developed an interview guide with questions for each topic area and selected SMEs accordingly. Based on a preliminary review of the literature and discussion among the research team, we identified six topic areas relevant to designing and evaluating record matching solutions:

- proposed matching solutions for the future;
- provider workflows, processes, and capabilities relevant to matching;
- vendor technical capabilities for adopting new matching solutions;
- provider value proposition and adoption factors (e.g., ability to integrate into workflow);
- patient value proposition and adoption factors (e.g., control of matching and privacy protection); and
- governance and engagement of stakeholders.

We identified SMEs through publications, recommendations from our professional network, and recommendations from other SMEs. We conducted each one- to one-and-a-half-hour interview over the phone, recorded the call, and summarized the key points discussed. In the interviews, we asked all SMEs to describe patient-empowered solutions for record matching; contextual factors, such as barriers and facilitators for various solutions to identify evaluation criteria; and suggestions for additional evaluation criteria that we could apply to a range of solutions. We also asked SMEs to recommend additional individuals and resources for further developing or identifying important solutions and evaluation criteria. A full list of SMEs is available in Appendix B.

Through multiple rounds of reviewing the literature extracts and interview summaries, we inductively developed a list of solutions and evaluation criteria.

Convening the Technical Expert Panel

The results of the analytic work above were gathered and shared with a group of TEP members. The TEP members were selected in consultation with the Pew team based on their expertise on a wide range of issues related to patient record matching. In selecting TEP members, we attempted to recruit representatives of the diverse stakeholders in record matching, including patients, providers, vendors, academic researchers, and government officials. We selected individuals who we believed would be capable of providing feedback on a diverse range of solutions. The TEP's role was to advise the research team. This approach complemented our SME interviews by giving a chance for different stakeholders to interact.

We convened the TEP for two one-and-a-half hour meetings on November 1, 2017 (Phase 1) and March 12, 2018 (Phase 2). Both meetings were held virtually. Prior to each meeting, we sent the TEP members a memorandum summarizing our findings. During the first meeting (Phase 1), TEP members discussed the work and provided comments that were used to update the evaluation criteria and inform our selection of a solution for further development.

Table 3.1. Technical Expert Panel Members and Affiliations

Member Name	Affiliation
David W. Bates, M.D., M.Sc.	Brigham and Woman's Hospital
Doug Fridsma, M.D., Ph.D., F.A.C.P., F.A.C.M.I.	American Medical Informatics Association
Andrew Gettinger, M.D.	ONC
Leslie Kelly Hall	Healthwise
Cora Han, J.D.	FTC
Adam Landman, M.D., M.S., M.I.S., MHS	Brigham and Woman's Hospital
David McCallie, M.D.	Cerner
Peter Szolovits, Ph.D.	Massachusetts Institute of Technology

Phase 2: Developing a Solution for Record Matching

In Phase 2 of the project, we used the information on potential solutions developed in Phase 1 to select a solution and further refine it. The solution we chose was actually a combination of proposed solutions investigated in Phase 1—one that involves using a patient's mobile phone or smartphone to "verify" his or her identity information and establish bidirectional communication between a patient-controlled smartphone app and a provider's health information system. Although the literature review and stakeholder engagement aspects of the research conducted in Phase 2 were structurally similar to Phase 1, they differed from Phase 1 efforts in several key ways (described below).

Targeted Document Review

Instead of a literature review, we reviewed targeted documentation cited by the SMEs during the Phase 1 interviews (e.g., *National Institute of Standards and Technology* [NIST] standards, *Fast IDentity Online* [FIDO] standards, and TEFCA documentation). These items were not formally abstracted, but information from the documents was used to inform the technology and governance considerations for our selected solution.

Expert Engagement

Key Informant Interviews

We focused our Phase 2 interviews on three topic areas relevant to developing and piloting a record matching solution that makes use of a mobile phone or smartphone and smartphone app:

- technology requirements
- application of evaluation criteria
- governance considerations.

We developed an interview guide with questions for each topic area and selected additional SMEs with expertise on these topics (some SMEs were the same as those in Phase 1). We identified these individuals through their publications, recommendations from our professional network, and recommendations from other SMEs and from TEP members (Appendix B). We also developed a working design document with preliminary use cases, workflow specifications, and questions for discussion, and we shared that document with several SMEs prior to the interview.

Convening the TEP a Second Time

Prior to the second virtual TEP meeting, we asked the TEP members to review a summary of our proposed solution. During the meeting and through written comments afterward, the TEP members provided feedback that we used to update the components of the solution and the plans for next steps. Following the second TEP meeting, we spoke with several additional SMEs (including two TEP members) to clarify remaining questions.

Limitations

This approach had several important limitations. First, we excluded several types of record matching solutions, as stated above, due to scope. These included improvements in algorithms used by matching engines and government-issued UPIs, which therefore were not compared to our included solutions. Similarly, we did not extensively investigate record matching approaches in other countries, but informal conversations did suggest that record matching requirements are shaped largely by health system structure and other idiosyncratic characteristics (country size, payment method) and that it may not be possible to import another country's solution without significant adaptation.

Second, we relied extensively on expert opinion on all aspects—identifying possible solutions to record matching, evaluation criteria, application of the evaluation criteria to the solutions, and selecting a solution for further development—rather than peer-reviewed research and data. Unfortunately, there was no way around this limitation because of the few assessments of record matching solutions involving patients that we found in our literature search. However, our experts included individuals with diverse perspectives and extensive experience and expertise in record matching. We hope that this work motivates further investigation into these solutions so that future assessments can provide additional evidence.

Third, although we included 32 experts with diverse perspectives, we may have missed important points of view from experts we did not include. Because this topic is complex and has not been the subject of much research, our selection of SMEs and TEP members likely shaped our findings and may have been biased in favor of their perspectives. Therefore, our findings should not be viewed as the final word on patient record matching and patient-empowered solutions. Rather, we hope it is the beginning of a more systematic dialogue concerned with

understanding the problem of record matching and proposed solutions, and we invite all interested stakeholders and commentators to scrutinize our analysis and selection of a promising solution.

Fourth, because there were a large number of solution-criterion combinations (110), we were unable to thoroughly investigate with our experts the application of every criterion to every solution. We gave our expert panel a chance to review our preliminary assessments and provide feedback, and focus on what we believed to be the most important advantages and drawbacks.

Finally, a solution that seems promising today may seem less so in several years. The landscape of health care has seen a rapid adoption of EHRs, emergence of various forms of HIE, extensive provider consolidation, and the advent of accountable payment models, among other changes. Consumer technology is changing even faster, with smartphone ownership increasing from 35 percent in 2011 to 77 percent in 2016 (Pew Research Center, 2018). Anticipating what kinds of record matching solutions make the most difference several years in the future is not possible to do with a high level of certainty.

4. Evaluation Criteria

Through literature review and expert input, we identified 11 evaluation criteria that are relevant to assessing the record matching solutions (described in Chapter Five), and to inform our selection of a solution, or cluster of solutions, for further development (Table 4.1). The criteria cover the potential for improving record matching if widely implemented, and several criteria are related to likelihood of implementation. Due to our interest in patient-empowered solutions, we include patient control as a criterion. We included privacy in five different evaluation criteria: in patient control, in terms of the extent to which the solution supports patient privacy preferences for record matching; in likelihood of adoption by patients, in terms of patient perception of privacy; in political viability, as it would be affected by privacy groups' perspectives; in minimal security risks, as they would indicate stronger protection against privacy violations; and in low potential for unintended consequences, in terms of enabling unwanted linking of data. For each criterion, we include a description and explain its relevance to assessing record matching solutions. These criteria are meant to be as comprehensive as possible but not mutually exclusive or independent. Rather, many criteria have complex interrelationships. We also include criteria even if they may not be easily measured quantitatively.

Table 4.1. Evaluation Criteria

1: Improvement in record matching if widely implemented
2: Patient control
3: Likelihood of adoption by patients
4: Likelihood of adoption by providers
5: Likelihood of adoption by vendors
6: Feasibility
7: Minimal security risks
8: Sustainability (operational and financial)
9: Political viability
10: Potential to foster new uses of matched records
11: Low potential for unintended negative consequences

Descriptions of Evaluation Criteria

Criterion 1: Improvement in Record Matching if Widely Implemented

In our evaluation criteria, we consider the extent to which the potential solution would reduce inter-institutional record matching errors if it were widely implemented. As this is the core focus of our work, we weighted this criterion highly in our assessments of potential solutions. Specifically, we assessed the solution's potential to reduce the rates of false negatives and false positives, relying on input from our experts. (Some solutions had the potential to increase the volume of data

exchange transactions, which is important, but our objective is more narrowly focused on improving match rates.) The experts we consulted disagreed regarding whether the goal should be to develop one approach that would be broadly applicable or to take a more piecemeal approach. One expert believed that the only hope for greatly improving matching was through a universal solution that would be used for all health care encounters. However, most believed that no one solution would address all patient record matching issues for all patients in all contexts; instead, they suggested that multiple approaches should be used. One expert said: "We're not thinking about *the* solution. We're designing a suite of solutions that have different benefits and drawbacks and finding ways to make all of that available to patients so they can pick what works for them . . . in a way that makes it easiest for their providers and for themselves." Several experts suggested that some patients will be more engaged in a matching solution than others, and no solution would engage all patients. One expert said that any large project will address most cases but will encounter edge cases that will lead to devastating consequences regardless of how comprehensive the solution attempts to be. We do not attempt to resolve this issue, but rather consider the extent to which each solution could improve matching with wide implementation.

Criterion 2: Patient Control

Our focus was to include record matching solutions that provided patients with a role in the record matching process, so we also considered the extent to which the solution provided that control. Degree of patient control could range from minimal (ability to opt-in or opt-out) to having at-will granular control over all record matching and data access among providers and the ability to view an audit log of all data activity.

Giving patients control over which providers have access to their data is controversial. In a series of studies, researchers in Indianapolis allowed patients to control which portion of their data from an HIE would be available to clinicians and staff within a clinic, with physicians having the option to "break the glass."[1] Most patients did not restrict access. However, a substantial minority did (45 of 105, or 43 percent), with many making use of fine-grained access control options, and a small number denying access to all doctors, nurses, and staff (Schwartz et al., 2015). The authors recommended the need for more education so that patients understand the implications of restricting access, and this point was also mentioned by several experts. Related work showed that many patients preferred having granular control of data and information about who accessed their records, but there was wide variation by type of information, recipient, and patient (Caine and Hanania, 2013; Caine et al., 2015). Previous studies of a personally controlled health record found patients had little awareness of data

[1] A "break-the-glass" request (which is named after breaking the glass of a fire alarm) of a patient's data would retrieve all of the patient's data including data the patient designated as private. It is meant to be used during an emergency when the patient is unable to consent to such a request, such as in the case of an unconscious patient.

sharing and access control functionality but high expectations for what it could do (Weitzman, Kaci, and Mandl, 2009; Weitzman, Kelemen, et al., 2012). Other studies conducted at the Regenstrief Institute in Indianapolis found that some providers used the "break-the-glass" functionality (even in situations that were not emergencies), and many providers believed that access restrictions would adversely affect care (Tierney et al., 2015). Several experts also expressed the concern that patients would restrict access to the detriment of their care, which would be a particular problem in the ED.

Researchers in separate studies identified many similar challenges with implementing granular access control capabilities, including keeping an updated list of provider types, which is required for role-based restrictions; changing patient preference over time; variability in institutional preferences; determining types of data that patients consider sensitive; effectively educating patients about consequences of withholding data; provider reluctance to share data; and technical considerations for structured and nonstructured (i.e., free-text) data in legacy systems (Goldstein et al., 2010; Meslin et al., 2013; Leventhal et al., 2015). Therefore, there may be an inherent tradeoff between offering patients control of their records and provider adoption. Despite these challenges, several experts felt that access to records must be controlled by the patient for them to trust the system. In addition, the experts said that the privacy settings must be simple for the patient to use and changeable when needed. In our evaluation criteria, we considered the degree to which a solution addressed these challenges and supported control and transparency over access and record matching by the patient.

Criterion 3: Likelihood of Adoption by Patients

Although there is considerable uncertainty as to whether patients would adopt any proposed solution, there was a rough consensus that very few patients are aware of current challenges with record matching and that most expect record matching to occur without their involvement. Therefore, any solution that requires the patients to change what they do would likely require that they receive some form of value above and beyond improved record matching. One expert suggested that any solution should be accompanied by a communication plan to help patients understand the importance of record matching and extent of the challenges. Patients will be more likely to use solutions that are simple, usable, require minimal effort, integrate with their existing daily workflows, and are easily understandable.

Concerning cost, there was some disagreement among experts. Some believed that many patients would be willing to pay a small fee to be involved with matching their own records, but others insisted that most patients would not, because they likely assume it is already occurring and view matching as a system responsibility that they are already paying for through service fees and premiums. Hence, it is possible that only wealthier patients would be willing to pay for a system that allowed them to improve their record matching.

Criterion 4: Likelihood of Adoption by Providers

Any solution to record matching will need to be adopted by providers. Several experts said that even small changes in workflow of front desk staff would be challenging, and that it would be easier if they could do the same workflow for all patients rather than needing to handle multiple workflows for different kinds of patients. That said, once the workflow is changed, it could likely be sustained. In this sense, there may be tradeoff between factors that improve adoption by providers (workflow consistency) and patients (ability to select among alternatives). Experts thought that providers would be motivated if the solution would allow them to be more efficient and reduce the number of staff needed for dealing with matching issues—or decrease fraud—but they are likely already accustomed to dealing with incomplete data from external sources, so they may not be willing to pay for improved cross-institutional matching. Some experts suggested that accountable care and value-based purchasing arrangements could create more incentive for adopting or paying for a solution, because a greater share of the costs and impacts on quality of a record matching error would be borne by the provider organizations. For providers who treat low-income patients, resources are more constrained, so the return on investment may be even more important. Government providers (e.g., Veterans Health Administration, Military Health Administration) may play an important role in adopting any solution, which would send a signal to the industry.

Criterion 5: Likelihood of Adoption by Vendors

Many solutions will require vendors to do additional programming. EHR and data-exchange vendors may be motivated to improve matching because it would reduce some of their costs. One expert suggested, however, that getting EHR vendors to make even simple programming changes can require long periods of time because of administrative delays in scheduling meetings with vendors. EHR vendors must adhere to federal certification requirements, which will likely take precedence over other efforts.

Criterion 6: Feasibility

Solutions that are more feasibly developed and implemented are more likely to improve record matching. We include feasibility of technical development and pilot testing, as well as considerations of the cost to develop the solution. (Ability to recoup ongoing costs and sustain operations are included in Criterion 8, Sustainability.) Although it may be challenging to assess feasibility of implementation without first developing the details of the solution, a preliminary assessment may be possible. For example, one study found that centralized storage of medical records would have better performances (i.e., faster access to data) at scale compared with distributed storage, which suggests that such a solution would encounter fewer implementation challenges (Lapsia, Lamb, and Yasnoff, 2012).

Criterion 7: Minimal Security Risks

Many experts insisted that any solution must be secure in the sense that it must produce few or zero errors, prevent unauthorized access to records by individuals who should not have access, prevent fraud, and be able to recover from errors or disasters that occur. For example, solutions that involve an assigned identifier may be able to recover from theft better than biometric-based solutions, because assigned identifiers can be easily replaced (Hieb and West, 2012).

Criterion 8: Sustainability (Financial and Operational)

Although it may be difficult to determine without pilot testing, any solution to record matching will require operational and financial sustainability beyond initial implementation. Any new stakeholder responsibilities must be manageable in the long term, and ongoing costs will need to be justified.

Criterion 9: Political Viability

Any solution must be politically viable and acceptable to stakeholders. Experts pointed out that a mandatory, government-issued health care identifier is an example of a solution that is not politically viable because the development and deployment of such an identifier was included in HIPAA, which was passed by Congress and signed into law in 1996, but the identifier has not been implemented as a result of resistance on the part of privacy advocates (Paul, 1998). A politically viable solution must be acceptable to those concerned about patient privacy (including privacy advocacy organizations) and have a reasonable chance of resulting in policy changes required to implement it. The *Fair Information Practice Principles* are standards for protecting privacy (Landesberg et al., 1998). One concern that privacy advocates may raise is that a matching system that begins as voluntary may end up becoming mandatory, as was the case with India's Aadhaar system in which a voluntary system for providing some government benefits became a nationwide system mandated for a wide range of purposes, including purchasing train tickets (Dixon, 2017).

Criterion 10: Potential to Foster New Uses of Matched Records

Some solutions were designed to facilitate innovations for matched data, and so we included this as a criterion, while acknowledging the considerable uncertainty for any given solution. Examples of possible innovations include tools that facilitate communication among patients and members of a care team, educational tools that help patients understand their health data, and the ability of patients to use the data for research or other secondary purposes.

Criterion 11: Low Potential for Unintended Negative Consequences

Risk of unintended consequences is inherent in any system change. While many of these risks are difficult to anticipate, we added this as a criterion in an effort to anticipate as many as

possible. Examples of unintended consequences include uninformed restrictions of access to records by providers, which might adversely affect care.

Chapter Summary and Analysis

The 11 evaluation criteria we identified reflect the complexity of the record matching design space and allow us to systematically consider the expected and unexpected effects of each solution. Record matching is a fundamental health system process, and one that intersects with multiple stakeholders, existing technical and socio-technical infrastructure, and economic incentives. To be comprehensive, an evaluation of potential solutions must use multiple lenses and understand nuanced tradeoffs. Some solutions may, in theory, improve match rates to near perfection, but not produce a return on investment for one or more critical stakeholders. Other solutions may suffer from feasibility, security, privacy, or political vulnerabilities, or fail to afford patients a meaningful degree of control over the process. We did not attempt to apply relative weights to each evaluation criterion (doing so would have been exceedingly difficult, given their complex interdependent relationships), but we did recognize that some evaluation criteria were likely to be more important than others for selecting a promising solution that enhances the role of patients in record matching. In the next chapter we apply the 11 evaluation criteria to our ten potential solutions.

5. Solution Alternatives and Assessment Using Evaluation Criteria

In our analysis of literature and expert input, we identified ten potential solutions to patient record matching, which are not mutually exclusive and may be combined in promising ways. (Table 5.1.) In these solutions, patients played one or more of the following roles (also indicated in Table 5.1):

- Patient gives provider additional identifying information to further distinguish the patient's identifying information from that of other patients.
- Patient gives provider information about medical record location to further distinguish the medical records from other patients' records.
- Patient verifies information used by provider for record matching to improve the data quality (e.g., fewer typos).
- Patient gives providers contents of records, obviating the need for providers to exchange that information.

Table 5.1. Identified Potential Solutions to Patient Record Matching and Patient Role

	Patient Role			
Potential Solutions	**Patient gives additional identifying information**	**Patient gives information about medical record location**	**Patient verifies information**	**Patient gives provider contents of records**
Solution 1. Implementing a VUID	X			
Solution 2. Using a public key as identifier	X			
Solution 3. Expanding the use of existing government-issued identifiers	X			
Solution 4. Adding knowledge-based identity information	X			
Solution 5. Adding the use of biometric data	X			
Solution 6. Having patient verify identity information			X	
Solution 7. Using consumer-directed exchange				X
Solution 8. Using health record banks	X			X
Solution 9. Having patients manually verify record matches			X	
Solution 10. Having patients supply record location information		X		

Below we summarize each solution from a functional perspective, such as how the patients and providers use it. For some, we include vignettes to illustrate core functionality. For these vignettes, we borrow from cryptographic conventions and use a patient named Jane and physicians named Dr. Alice and Dr. Bob. Then, after describing each solution, we present summaries of our application of the evaluation criteria. The result of our systematic application of every criteria to every solution (110 applications) is summarized in Tables E.1 and E.2 (Appendix E). For purposes of readability, in this chapter, we focus on criteria that were most salient or for which the literature or experts provided feedback. As we note in the text and tables, for many solutions, the assessment of some criteria are unknown or highly speculative. We have drawn extensively on the experience on CommonWell Health Alliance because it has experimented with multiple methods for improving inter-provider record matching.

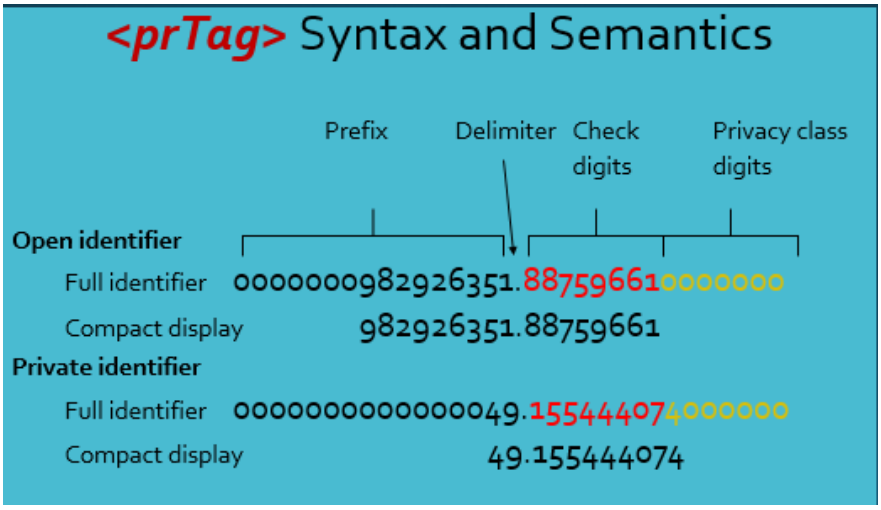
Identified Solutions

Solution 1: Implementing a Voluntary Universal Identifier

The idea of a UPI is perhaps the most discussed solution to patient record matching (HHS, 1998). This solution has been proposed in recognition of problems with using Social Security numbers, such as privacy concerns arising from their facilitating linkages with financial and other data, increasing opportunities for fraud and identity theft, and clerical errors due to the lack of automated error-correcting techniques, such as *check digits* (i.e., identifier digits that are computed by the other identifier digits so that typos would likely produce invalid identifiers). In prior work, RAND investigated the costs, benefits, political issues, and privacy implications of a UPI issued by the federal government for use by patients for the duration of their lifetime, similar to a Social Security number (Hillestad, Bigelow, Chaudry, et al., 2008). In short, the research found that a national implementation would cost roughly $11 billion; the benefits are more difficult to quantify but would probably justify the costs; and such an identifier would likely improve privacy by reducing the need to share as many patient attributes for record matching. However, the UPI was blocked by Congress due to privacy concerns. Here we describe an implementation of a *voluntary universal identifier* (VUID) that is not issued by the federal government (although any trusted organization could potentially serve as the issuer). Unlike some other solutions we consider, extensive details are available because this type of identifier has been developed over several decades. We summarize the core functionality.

The identifier-based matching solution we describe was developed as part of an *American Society for Testing Materials (ASTM) standards* process in 1995 (Hieb, 2010), and an implementation of this solution was supported by Global Patient Identifiers, Inc. (GPII) (“GPII, Inc.,” 2013). In that implementation, the identifier is called a <prTag> (which stands for “patient record tag”) by GPII and is 32 digits long (Figure 5.1).

Figure 5.1. GPII Identifier



SOURCE: GPII, used with permission.

GPII's implementation includes more functionality than simply issuing a unique identifier: it involves a central service that can verify that an identifier is unique and valid, invalidate and replace an identifier that has been compromised, generate a list of locations in which an identifier has been used (i.e., a record-locator service), link multiple "private identifiers" that can be used to segment data for privacy and access control, support a "break the glass" request to allow a provider to locate all of a patient's records regardless of segmentation, verify check digits, and other functionality. The central service reduces security risks by not storing any patient demographic information centrally, only a list of identifiers and their associated locations. The central service also does not provide a mechanism for the actual exchange of data, so other data exchange methods would need to be used. This solution was developed with the goal of supporting identification and record matching in all medical encounters, and to create the minimal functionality needed to accomplish that goal in a way that could be adapted to respond to potential problems.

Health care providers' front desk staff are responsible for issuing the identifiers to patients and managing any other operations (e.g., merging two identifiers inadvertently issued to the same patient). The central service requires that each provider install its software and hardware, which interfaces with the *master patient index* (MPI) of the provider's EHR. The front desk staff would use software that is customized to the workflow for each use case in the form of decision trees (e.g., patient has an identifier already, patient forgot his or her identifier and should receive a temporary one). In a typical case, the front desk staff would issue a new identifier to a patient who does not yet have one by requiring some form of identity-proofing (e.g., patient shows a government-issued identifier and calls an identity-proofing company to answer some additional questions). In all subsequent visits, the patient would need only to show his or her identifier and verify some demographics. (See Vignette 1.)

Vignette 1: Voluntary Universal Identifier

Jane shows up to an in-person appointment with Dr. Alice. A staff person at the front desk offers Jane the option to have a unique identifier issued to her. She accepts and then goes through an identity-proofing process by showing the front desk staff her driver's license number and calling an identity-proofing agency. (Identity-proofing can occur in other ways as well.) Upon completion of this process, she is given an identifier printed on an ID card. (The central service issues the number, and the provider can give the number to the patient on paper or in the form of a smartcard, smartphone app, or something else.) For all future visits to that provider, Jane presents her identifier, thereby facilitating check-ins and helping front desk staff find the correct record.

When Jane visits a new provider, Dr. Bob, she gives the front desk staff her identifier, which is then used to retrieve from the central service a list of the patient's previous providers. The software also automatically downloads the patient's demographic information from Dr. Alice's office. Dr. Bob's office is then added to the central service's list of locations associated with the patient's identifier.

If Jane decides she wants her data from Dr. Bob's office to be unavailable to any other provider (perhaps because Dr. Bob's office contains sensitive mental health data), she can request that the front desk staff issue her a "private identifier," which the central service would link to her "open identifier." Jane could share her private identifier, and thus her sensitive data, with any provider whom she chooses. Any provider could also choose to "break the glass" and find out the list of all record locations. Nothing prevents patients from creating multiple open identifiers, but doing so would defeat the purpose of facilitating matching. If that happens inadvertently, a front desk staff can merge two open identifiers.

Evaluation of Solution 1

Although this solution would greatly improve matching if adopted and although it offers additional functionality for patient control and resilience in the event of a security compromise, there is substantial uncertainty that providers or patients would adopt it.

[Improvement in record matching if widely implemented] If adopted and used as intended, this solution would match records used by the same individual perfectly.

[Patient control] This solution would allow patients to segment and control access to their records.

[Likelihood of adoption by providers] For providers, the major barrier is the requirement to install new software and hardware and add new responsibilities for front desk staff to manage the identifiers and deal with issues that arise. Such an effort would require a major change in

workflows. CommonWell Health Alliance's experience asking front desk staff to record government-issued identifiers in patient registration systems found that getting clinic personnel to complete these tasks was a huge barrier to adoption. Although there would be a central entity providing hardware, software, and a list of active and inactive identifiers, the responsibility to manage the identifiers would be diffused among existing health care providers. If there is uneven provider involvement in managing identifiers, some providers may find themselves cleaning up problems with the identifiers (e.g., merging multiple identifiers, splitting incorrectly merged identifiers) stemming from other providers who are not correctly following protocol. For the system to work effectively, providers would need to trust that other providers are using the system correctly. If the federal government took responsibility for managing the identifiers, some of these problems would be avoided, but this solution would require that some stakeholder pay for the hardware and software, identity-proofing, and other identity management responsibilities, and would be questionable from a political viability standpoint.

Providers may also be hesitant to engage in this system for two other reasons. First, they may be reluctant to establish a dependency on a central organization for an ongoing operational need. There was some consensus among our experts that, if a voluntary unique identifier is used, it must be issued by one central entity because otherwise a patient may need to be matched between entities, which adds complexity and potential for matching failures. Therefore, having record matching processes depend on one institution may be unavoidable for this solution, but it could still be a potential obstacle. Second, providers may not want to replace existing methods for patient registration and record location if they have made significant investments in them, especially given uncertainty as to its ultimate success.

[Likelihood of adoption by patients] Patients may go along with receiving identifiers if prompted by providers. In the only pilot test of this solution, which was cut short due to the failure of an HIE, providers issued more than 200 identifiers to patients. However, it is unknown if most patients would remember to bring them to subsequent provider visits and use them correctly (e.g., maintain only one "open" identifier).

[Sustainability] It is also unclear who would cover the costs of this solution or the identity-proofing required. Options could include an encounter fee paid by the provider, or an issuing fee paid by a patient's insurance company, but the business model is uncertain. Proponents of this solution suggest that the costs would be recouped in the form of reduced matching errors (a claim made for other proposed solutions we identified).

[Feasibility] Although use of private identifiers would protect privacy by allowing patients to segment their data, many of our experts were skeptical that patients would be able to keep track of multiple identifiers, even if they were motivated to do so. Also, as the Regenstrief studies show (Schwartz et al., 2015), there are still major challenges in implementing data segmentation in a way that is acceptable to providers, and many providers may be reluctant to adopt a solution that allows patients to easily hide important data from them without fully understanding the

consequences (Goldstein et al., 2010). As in those studies, some providers may insist on "breaking the glass" for every patient, which defeats the purpose of data segmentation.

The next step to advance this proposed solution is a pilot test that assesses providers' ability to integrate a VUID into routine workflows and patients' long-term usage. Such a pilot test would help determine the magnitude of the barriers we identified, which would otherwise remain unknown. We believe that a pilot could be conducted without additional standards development work because a version of this solution has already gone through such a process. However, piloting would require several provider organizations with shared patients to change their operational workflows, and we expect that most would be reluctant to do so unless they viewed this solution is having a high likelihood of long-term success and widespread adoption.

Solution 2: Using a Public Key as Identifier

Another identifier-based solution that was suggested in expert discussions and the literature but not described in detail would involve utilizing *public key cryptography* (Szolovits et al., 1994). The patient would be issued a *public key*–private key pair, and the public key would be used for record matching as a piece of identity information. At each encounter, the patient would be able to use the private key to prove that the public key belonged to her (presumably using a smartphone app at check-in); this step would provide additional assurance of identity beyond what was provided in Solution 1. However, unlike the case of Solution 1, the keys would not be human friendly (i.e., they would be too long to be memorized or recited in a few seconds). Use of the key would provide extra security against theft, above and beyond what would be afforded by a human-friendly identifier and would guard against typos. The public key would be used as an additional identifier in record matching engines when providers exchange health records. Patients wishing to segment their records, to allow provider-specific sharing decisions, could do so using multiple keys. This solution would require standards governing the public key–private key pairs.

In our analysis, we identified two possible methods for implementing this approach. First, patients would be responsible for generating and managing the keys and could do so without a central organization. Second, a central organization would issue the keys after patients had gone through an identity-proofing process.

Evaluation of Solution 2

[Improvement in record matching if widely implemented] The use of public keys as identifiers, if used consistently, would greatly improve record matching, much as any unique identifier would.

However, there are many open questions regarding this potential solution. What organization, if any, would be responsible for issuing and managing the keys? Who would handle such situations as patients losing their corresponding private keys or the keys becoming compromised? What benefits would motivate patients to adopt a key and use it consistently? Who would pay for development and ongoing operation? How would providers change their workflows to accept

these new identifiers? Because these questions are unanswered, we do not consider this to be a complete solution; rather, it may serve as a component of other solutions.

Solution 3: Expanding the Use of Existing Government-Issued Identifiers

Critics of issuing a national patient identifier often point out that U.S. citizens already keep track of and maintain many other identifiers, and suggest that some existing identifiers could be reused for purposes of record matching. Although Social Security numbers are problematic for reasons listed above, other government-issued identifiers, such as driver's license numbers or passport numbers, are universally unique, require rigorous identity verification to obtain, and are already routinely checked by front desk staff at many health care encounters for purposes of identity and insurance verification. More than 70 percent of individuals over the age of 20 have a driver's license (Sivak and Schoettle, 2016). If such an identifier is included as an additional piece of identifying information for purposes of matching, it would have the potential to improve match rates. CommonWell Health Alliance (a vendor-based HIN) has pilot tested this approach. In that network's method, front desk staff were expected to type the government-issued identifier into the appropriate field in the patient registration software; a *hash* of it is stored centrally and used to link records.

Evaluation of Solution 3

[Improvement in record matching if widely implemented] This solution has strong potential to improve record matching if widely implemented because government-issued identifiers have good qualities for record matching, including uniqueness and strong identity-proofing. However, it would not completely solve the matching issue because patients may not necessarily use the same government-issued identifier at every health care encounter. In addition, the primary government-issued identifier we considered, the driver's license number, is issued by states so when patients move to a different state, their form of identifier could change.

[Likelihood of adoption by patients] Barriers for patients would be minimal: A large number of patients already has government-issued ID (though not all) and already present them to their health care providers, so it would require minimal change for most patients.

[Likelihood of adoption by providers] For providers, on the other hand, although many are already checking government-issued IDs at the point of care for purposes of identity and insurance verification, the experience of CommonWell Health Alliance suggests that the additional workflow requirement for front desk staff to enter a number into their patient registration software is cumbersome and challenging to implement, especially with high turnover rates among front desk staff. In addition, unless the government-issued identifiers have check digits, typos would likely be a problem.

Solution 4: Adding Knowledge-Based Identity Information

Knowledge-based identity information includes additional identifiers that could be collected and used for record matching. Examples of knowledge-based data elements include mother's maiden name, make and model of first vehicle, and birth city. These would be implemented in the form of challenge phrases that are asked of the patient at each encounter and used by matching engines. Knowledge-based approaches are commonly used for authentication in settings within and outside of health care, but not for record matching to our knowledge. Using this solution would require questions to be standardized and the same questions to be asked of each patient. Some patients may deliberately use fake answers to avoid releasing information that is used for authentication in other settings. As long as they used the same fake information in each setting, matching would still be improved.

Evaluation of Solution 4

[Improvement in record matching if widely implemented; likelihood of adoption by patients; likelihood of adoption by providers; feasibility; minimal security risks] This solution may improve record matching somewhat if it were widely used and if the knowledge-based questions were relatively unique. However, it could face major challenges, including required changes in workflows for providers, potentially inconsistent responses from patients due to forgetting answers, security concerns from making more widely available the types of questions currently used for identity-proofing and authentication, clerical errors, and issues with standardizing knowledge-based data elements.

Solution 5: Adding the Use of Biometric Data

Biometric data may include fingerprints, iris scans, facial recognition, palm scans, genetic testing, or voiceprints. Technical standards that define characteristics of "raw" biometric data captured by devices have been established by the National Institute of Standards and Technology (NIST) for fingerprints, iris scans, and facial recognition. Vendors compete in developing devices for capturing standard-conformant biometric data in a user-friendly manner, and use proprietary biometric templates (representations of the standardized biometric data) and matching algorithms that operate on the templates. (Applying the matching algorithms directly to the biometric data instead of a template would be more expensive and time-consuming from a computational perspective, and would require greater availability of the more privacy-sensitive biometric data. Templates are less privacy-sensitive because they could be replaced; the original biometric data cannot.) The various types of biometrics have advantages and disadvantages in terms of convenience, cost, security, and matching performance (Hembroff, 2016; Leonard, Pons, and Asfour, 2009).

In our discussions with experts, we found that there are three distinct uses of biometrics that are often conflated but important to distinguish:

1. *Locally, on a secure personal device*: In this way, the biometric information such as a fingerprint is stored on the device in encrypted form. When a person uses his or her biometric information to unlock the device, it is compared with the already encrypted data. In this implementation, it would be impossible to reconstruct the biometric in a form that could be reused for other purposes ("iOS Security," 2018). Many devices offer this capability, and consumers are increasingly comfortable with it. Emerging FIDO standards enable individuals to use biometrics on a local device in place of entering usernames and passwords on multiple apps or websites ("FIDO Alliance," 2018). However, this use of biometrics by itself does not improve cross-institutional record matching.
2. *Locally, within a single institution*: This is how some health systems currently use biometrics. Biometric data in the form of a template is stored as part of the providers' registration software. When a patient comes to the front desk, her biometric is captured and used to look up her record in the registration software. Many patients use this method when it is offered by providers. This use of biometrics may improve record matching within provider organizations, such as by reducing duplicate records, but would not directly improve cross-institutional record matching.
3. *Shared, across multiple institutions*: In this way, either the original biometric data (e.g., iris scan image), a template, or some other representation of the data would be shared among providers and used directly in cross-institutional record matching. To our knowledge, no organizations are routinely sharing biometric data across provider institutions for purposes of record matching, although experiments are underway.

The last use of biometrics is most directly relevant to our interest in improving cross-institutional record matching. Although we did not comprehensively survey all current activities that employ biometrics for this purpose, we identified two general approaches for potential solutions in which biometric data play a role.

In the first approach, raw biometric data (or some standardized representation of it) would be included in identity information along with existing demographics. Under this option, patients would have their biometric data captured at each point of care, and it would be used by record matching engines as an additional identity attribute. (Record matching engines would likely convert these data into a template to improve speed of computations.) It is likely that this option would benefit from leveraging NIST standards, but it is also possible that new technical standards would be needed to address requirements of this application, which may be different from those for which the NIST standards were developed (e.g., cost of devices, matching accuracy, computational performance). Existing technical standards for data exchange would need to be updated to incorporate biometric data ("Cross-Community Patient Discovery," 2017). See Vignette 2 for an example.

In the second approach, which could build upon the first, a more complex technical architecture would be established in which the capture and use of biometric data would be synchronized across health care providers. Multiple architectures may be possible, and to our

knowledge little work has been done to investigate the options. A primary purpose of this more elaborate infrastructure would be to provide additional privacy and security safeguards for the biometric data. In ongoing work in South Africa, developers are experimenting with a decentralized database that could be implemented incrementally with mechanisms to allow compromised biometrics to be designated as such and no longer accepted within the network of providers (e.g., an individual's thumbprint would no longer be used to match that individual's records). Other possible technical architectures may include use of a centralized entity that stores the biometric information. To became widely adopted, the software for such technical architectures may require some kind of new incentive or certification.

For any use of biometrics to improve record matching, the same type of biometric must be collected at multiple locations in a common format. For example, a patient's thumbprint provided to one provider cannot be matched with that patient's iris scan by another provider unless a third organization has access to both the thumbprint and iris scan. Best practices would be needed to ensure that the data are captured in a consistent way within workflows across the health care system.

Privacy and security of biometric data could be protected through promotion of best practices (e.g., storing the raw biometric data separate from other data sources, splitting individual biometric data into multiple databases). For example, devices or processes may be certified by some authority for adherence to security protocols.

Vignette 2: Biometric-Based Identifiers

When Jane visits Dr. Alice, the front desk takes a picture of her face in a way that conforms to technical standards. The picture is incorporated into Jane's list of demographic data. In order to bring up her record in future visits to Dr. Alice, Jane would always have her photograph taken (which would be timestamped so the more recent photograph would be easily identified as her appearance changes over time). When Jane visits Dr. Bob, she also has her photo taken. Any time records are exchanged between Drs. Alice and Bob, the photographic data are used by the matching engine to improve the odds that a correct match will occur.

Evaluation of Solution 5

We discuss identified tradeoffs in terms of several salient evaluation criteria. Because biometrics is a complex domain, this analysis provides only highlights and should not be considered comprehensive.

[Improvement in record matching if widely implemented] Experts agreed that biometrics would enhance the performance of matching engines because of their relative uniqueness

compared with demographic information; moreover, their performance will likely continue to improve, given that biometric capture and matching are the subject of active research and technology development. However, every individual biometric has some limitations (e.g., facial recognition does not work as well for certain minorities and children; fingerprints are less effective for the elderly), except perhaps genetic information, which is cost prohibitive to attain at every encounter. When being compared across large datasets, individual biometric data types are likely insufficient to uniquely identify individuals, but they may be sufficient when combined with demographics and used with other biometric data types. In NIST competitions, for example, iris scans were found to have false negative rates of approximately 0.2 percent (when the false positive rate was set to one per million). Fingerprints could achieve rates of 0.1 percent with all ten fingers, and lower rates when fewer fingers were used.

[Likelihood of adoption by patients] Many experts agreed that devices that quickly and easily captured biometrics would be used by most patients and could be used even when the patient was unconscious or had dementia and did not remember his or her name. Some experts suggested that concerns about privacy had diminished, since the population has already become accustomed to this type of data for authentication in various contexts, and that most individuals would feel comfortable with this new use for it.

[Likelihood of adoption by providers] Although biometrics readers have already been adopted by some providers for finding patient's local records, some experts suggested that the cost of biometric technology (particularly for devices that capture the data in a user-friendly manner, which does not require multiple scans or ideal input conditions) may be prohibitive, especially for safety net providers. Some experts suggested that benefits to reduced cost in record matching would recoup the costs (a claim made by experts about several of our proposed solutions) and that the cost of the technology may decrease over time.

[Minimal security risks] Although the presence of biometric data does not inherently make a system more vulnerable, some of our experts believed that the increased collection and sharing of biometrics may result in an increased target for hacks and interception, and that exchanging data between entities increases chances of those data being compromised. On the other hand, if the biometric data were also used for authentication, it could prevent unauthorized access.

[Potential for unintended negative consequences] The consequences of using an identifier that could not be changed was perhaps the most contentious issue we discussed with experts. Experts with privacy concerns believed that increasing use of biometric data would open up the possibility for them to be used for new unforeseen purposes, such as facilitating linking with law enforcement or other databases against patients' wishes. Proponents of biometrics pointed out that some demographic data (e.g., name, date of birth), while technically replaceable, are not often done so in practice and therefore not much different from biometrics in this regard. Also, individual biometrics are not uniquely identifying, but rather need to be combined with other data (or multiple biometrics), which may mitigate some concerns of the consequences. Technical and administrative safeguards can also mitigate problems with stolen biometric data (e.g., disabling

specific biometrics for specific individuals within an organization or network, restricted use to in-person settings, "liveness" checks to verify that the biometric data is possessed by someone who is alive). However, it is unknown if the data will be used only in the context of these approaches in the future. It is possible that the more complex technical architectures we identified in the previous section may address some of the concerns with biometrics, but to our knowledge, these have not been considered by health care stakeholders beyond informal discussions.

[Political viability] Greater use of biometrics may face legal and political challenges. Changing laws surrounding biometric data collection and variation of laws by state may create barriers to exchanging them (Chew and Ball, 2018). More broadly, attempts to harmonize or loosen those laws may meet resistance from privacy advocates. Some of our experts believed that current legal protections are inadequate to prevent unwanted use of individual's data, as evidenced by leaks and privacy violations in health care and other sectors, and believed better protections were needed before allowing more widespread use of biometrics.

Solution 6: Having Patients Verify Identity Information

In our analysis, experts suggested that the data quality of some types of identifiers could be improved by verifying the patient's possession of the identifier. For example, mobile phone numbers or email addresses can be verified by sending a one-time code or link. These identifiers are universally unique (although an individual can have more than one), and many providers already collect them. Phone numbers in particular have qualities that are helpful for record matching: They are unique, actively managed by a coordinated group of established companies that adhere to international standards, and change infrequently; moreover, patients have strong incentives to maintain them. The verification step would improve the quality of data used by matching engines by reducing typos, and would ensure data is entered into correct fields (e.g., number in mobile phone field is an actual mobile phone, not a landline), thereby improving the matching engines' performance. Furthermore, once verified, a *metadata* tag would be applied to the identity information to indicate to matching engines that these fields are more likely to be accurate.

A mechanism for transferring verified identity information to providers was proposed by the Workgroup for Electronic Data Interchange (WEDI), a coalition of health care stakeholders, as part of a Virtual Clipboard Initiative (WEDI, 2016). The method and details for performing the verification were not specified. The goal of this effort was to "define a set of industry standards for exchanging and securing health care information within mobile applications used by patients and/or their advocates" (p. 5) with the intention of reducing administrative clipboard-related burdens on patients and providers, improving patient identification at the point of care, and streamlining the insurance eligibility processes. The initial planned development and pilot were expected to allow patients to share the information on their insurance card with their providers. Unfortunately, the effort stalled due to lack of continued support, and the pilot was not launched.

Evaluation of Solution 6

[Improvement in record matching if widely implemented] This solution has strong potential to improve record matching, especially if data elements that are unique, such as mobile phone numbers and email addresses, are used. Currently, mobile phone numbers and email addresses are collected by many providers, but they may have typos, or may be entered into the wrong fields (e.g., mobile phone number entered as a home phone number). Some record matching engines may already use these data elements, but matching rates could be improved if these data were more routinely collected and verified as accurate.

[Likelihood of adoption by patients; likelihood of adoption by providers] Performing some degree of validation may be possible with minimal additional effort on the part of patients or providers, such as sending verification messages to patients via text message or email and asking them to respond or click a link to confirm. Somewhat stronger verification may require some additional effort on the part of patients and front desk staff at the point of care, such as using a one-time passcode that the patient tells the front desk staff to enter. This kind of verification is commonly used in the financial industry and other sectors for authentication (albeit not often in person), so patients will likely be familiar with the process.

However, these data elements are not perfect for matching. Mobile phone numbers sometimes change (we could not find estimates of frequency) and are not universal (though adoption is very high). Not all patients have email addresses, and some use multiple ones. For children or patients who are incapable of using phones or computers, parents' or caregivers' identity information may be used for the patients, in which case they should be labeled as such. Because these data elements are considered to be another attribute in matching engines and not unique identifiers, the fact that multiple individuals have the same attributes may not be problematic from a record matching perspective—name, gender, date of birth, or other attributes can help distinguish patient from caregiver/parent.

Solution 7: Using Consumer-Directed Exchange

The goal of consumer-directed exchange is to allow patients to access their health records and share it with any applications, organizations, or individuals they choose. ("Consumer-mediated exchange" and "consumer-directed exchange" are sometimes used interchangeably. We define *consumer-mediated exchange* as including any types of data exchange, including exchange through *health record banks* [HRBs], in which patients control their records and share them with providers.) The CARIN Alliance is an effort to unite industry leaders in advancing the adoption of consumer-directed exchange (CARIN Alliance, 2017). Although improving record matching is not always mentioned by these efforts as an explicit goal, this type of exchange may allow patients to give the contents of their medical records to their providers, thereby changing the workflows in which record matching is performed.

Consumer-directed exchange focuses on helping patients aggregate all of their health care data into one application. This likely requires reliable identity-proofing and authentication to make sure that the patient doing the aggregation is in fact using his or her own identifying information and not trying to access someone else's records. Some efforts are exploring methods for standardizing identity-proofing processes and universal 2-factor (U2F) authentication so that they would be less cumbersome for patients (i.e., could be done remotely). Once a patient has identity-proofed and authenticated him- or herself there might be three methods for aggregating data via a third-party application: querying specific providers or HIN networks, which would use matching engines to find records; accessing publicly available API end points that allow access to provider data sources; or allowing the patient to more easily log in to the providers' patient portals and download them. (See Vignette 3.) Additional workflows would need to be established to allow the patients to share their aggregated records with providers. Provider-to-provider record matching would no longer be needed for patients who used this method, but record matching would need to occur between the patient-controlled account and EHRs in two places: when patients aggregate their records by querying a network for providers, and when patients shared their records with their providers.

Vignette 3: Consumer-Directed Exchange

Jane wants to assemble her health record from all previous providers. She hears about a software company that will let her do this, so she signs up with a username and a password or alternative authentication methods (e.g., U2F) and downloads the app on her smartphone. The app asks her to go through a remote identity-proofing process to confirm she is in fact Jane by submitting a picture of her driver's license and a picture of herself, and answering some question about her finances. Jane is then asked by the app to specify the regions in which she has received care. She enters the towns of her providers, or their clinics' names if she remembers, and the app queries every provider in those regions using her identity information (name, date of birth, address) to look for a match. For any matches that are found, the app uses standard Application Programming Interfaces (APIs) to the EHRs at each location and retrieves all of Jane's data without requiring her to establish a patient portal at each clinic. If records for her visit to Dr. Alice are not discovered using this method, Jane can use her app's login credentials to log in to Dr. Alice's patient portal and download her records. Jane can use the data in whatever functionality the app supports, which may include education tools, or share the data with other apps or with Dr. Bob if he accepts it. Dr. Bob would need to link the data from Jane's app into his clinic's patient portal, which may be facilitated by the front desk staff when Jane comes to the office for a visit.

A research project conducted from 2007 to 2009 demonstrated some of the functionality needed to implement consumer-directed exchange and integration into providers' EHRs (Mandl et al., 2007; Bourgeois et al., 2009). Private sector examples (which vary in functionality) include Dossia, Google Health (which discontinued in 2011), Microsoft Health Vault, Apple's Health Records, CareEvolution, b.well, MedFusion, and PatientLink. Some experts discussed the use of blockchain to implement functionality similar to consumer-directed exchange; in this scenario consumers would use data stored on a blockchain to control access to their medical records. The blockchain would function as a distributed database that removes the dependence on a central organization while providing assurance that the data was not tampered with. (See Appendix F for more details.)

Evaluation of Solution 7

The idea of an aggregate health record under the patient's control was viewed by many of our experts as the ideal solution for patient record matching, as well as many other problems in the health care system.

[Improvement in record matching if widely implemented] Because the patient would give providers the actual contents of the records themselves, there would not be any need for matching engines. However, matching errors could still occur: Patient queries to aggregate their records would rely on existing imperfect matching engines, and when patients shared their records with providers, those records may not always be matched to the correct record in the EHR.

[Patient control] This solution would still raise questions about patients' control of their own data. Some experts insist that patients should be given complete granular control over their data to share or not share with any providers of their choice. However, the Regenstrief studies paint a more complex picture (Schwartz et al., 2015). Most patients do not understand the consequences of "hiding" certain aspects of their data from their providers, and without education many patients would likely make mistakes that they may regret. Providers are highly skeptical of giving patients such control, since it could impede their ability to give patients quality care, reduce quality scores and reputations, interfere with the relationships with their patients, and make the practice of medicine more frustrating. Some of these concerns may be ameliorated by carefully designed PHRs that educate patients and enforce strict rules related to data sharing. However, to our knowledge, such best practices do not exist currently.

[Likelihood of patient adoption] Experts pointed out that relatively few patients are actually interested in managing their medical records and would prefer to delegate this function to their providers. However, some experts were more optimistic and pointed out that there is a growing number of digital health companies developing innovative uses for health data, which may provide an additional value proposition for patients and increase interest. Recent technical standards for data format and communication can facilitate integration of EHRs with PHRs ("Blue Button," 2017). Also, adoption of APIs due to federal meaningful use requirements

and the 21st Century Cures statutory requirements may make this solution increasingly feasible (Public Law 114-255, 2016). Some experts were enthusiastic about Apple, Inc.'s recent release of a PHR, which allows patients to have relatively easy access to their own health care data from a mass consumer platform (Kohane, 2018).

[Likelihood of provider adoption] Even if patients do manage to aggregate their medical records in a PHR, the workflows and technology that would allow providers to use that health data are not in place. Some of our experts suggested that providers may not be interested in managing a new channel of health data from patients because it may be of variable or uncertain quality and may further complicate their already complex workflows. Providers may prefer to receive data only through existing channels, such as HINs, which may not be complete or may have other data quality issues but are at least familiar sources of information.

[Sustainability] There was a strong acknowledgment among experts that previous attempts have failed, and there is no clear pathway toward achieving this vision. We are unaware of a business model that can make this solution sustainable. Some of our experts insisted that creative entrepreneurs would figure it out and dismissed the question of a business model as an irrelevant concern. (However, because PHR companies would not be covered entities under HIPAA, there may be a risk that they could be tempted to sell patients' data to others, even against patient preferences for privacy.) Others suggested that high-deductible health plans would motivate patients to use these kinds of services to keep better track of their medical data so that they would get more out of the visits they pay for, and accountable care efforts would create incentives for providers to use data from patients.

Solution 8: Using Health Record Banks

Health record banks (HRBs) have been defined as "independent organizations that provide a secure electronic repository for storing and maintaining an individual's lifetime health and medical records from multiple sources and assure that the individual always has complete control over who accesses their information." The HRB's role is to "automate the process of managing and reconciling the EHR data for the consumer" ("Health Record Banks FAQs," 2016). HRB proposals tend to assume that there would be one HRB for a given geographic region and that most providers in that region would participate (Mantravadi, 2016). One expert described HRBs' sole job as compiling and curating records on behalf of patients in a form that could make sense of a longitudinal record. In this way, the records are matched and aggregated when the records are created, in advance of when they are needed. Although not directly relevant for record matching, HRBs would also allow patients to contribute data themselves from wearables (e.g., activity monitors) and genetic testing, as well as data about their medications through portals linked directly to the HRB. Proposed models suggest that HRBs may provide an app store that allows third-party applications to be installed and provide innovative functionality with patient health data that could engage both patients and providers. To improve record matching, HRBs

may issue new identifiers to patients, which the patients would then give to their providers in subsequent encounters. This would be similar to the VUID approach described above, except that the health records would be stored centrally. See Vignette 4 for an example of how an HRB might work.

Although discussions of HRBs often assume that they are independent of providers, one demonstration project was implemented within a provider organization (Weitzman, Kaci, et al., 2011; Mandl et al., 2007). However, one expert suggested that using a provider organization to host an HRB was unlikely to become widely adopted because of competitive resistance among providers to release their patients' data to another provider, and that providers would more likely trust a third party (i.e., not a health care provider) as the HRB to prevent competitors from accessing each other's data without legitimate reasons. Financial institutions, such as credit unions, could also potentially host an HRB. However, that could also pose a risk of such institutions using health data in their financial decisions, such as mortgage approvals.

Vignette 4: Health Record Bank

Jane signs up for an HRB through a private company that covers her region, and she is asked to go through an identity-proofing process at a participating provider or remotely. As in the process she goes through when she signs up for a regular bank account, she understands that this process is necessary to go through one time in order to keep her records organized, secure, and available to all of her providers. The HRB issues Jane a unique identifier that she can use whenever she receives care. Later that week, Jane goes to a new provider, Dr. Alice. She gives Dr. Alice her HRB identifier, which allows Dr. Alice to view her health record. After the visit, Dr. Alice's record is automatically added to the HRB, and the HRB makes sure the new data is incorporated in a way that makes it understandable for subsequent visits. A few weeks later, Jane visits Dr. Bob, another new provider, who orders an imaging test. Jane has the imaging test done later that week, and the imaging center sends the result to the HRB. The HRB receives the record and is responsible for making sure it is matched to Jane's account (using a combination of matching engines and human adjudication).

Evaluation of Solution 8

HRBs share many characteristics with consumer-directed exchange and have similar advantages and disadvantages. But HRBs are different in that they would evolve from a regional initiative and more direct relationships with providers rather than with patients. One expert suggested that regional HIEs may evolve into this solution, but none to our knowledge has

directly signed up patients or issued identifiers to them. However, many HINs keep identifiers internally, and some have begun sharing them with participating providers to improve internal record matching capabilities ("MiHIN," 2017).

[Improvement in record matching if widely implemented] For patients who use HRB-issued identifiers as expected, this solution would greatly improve record matching. For patients who do not use such identifiers, the HRB would be responsible for record matching but it is unknown how effective it would be or what additional methods it would use.

[Likelihood of patient adoption] It is unknown the extent to which patients would use an HRB. It would likely depend substantially on specific HRB implementations.

[Likelihood of provider adoption] Provider value proposition is also a challenge. Consistent with expert input on other solutions, one expert suggested that the willingness of providers to support an HRB model would grow because access to data would help reduce costs from redundant testing, which is a source of profit today under fee-for-service payment methods but will be lost revenue under emerging accountable care arrangements. These changes in incentives may generate needed support from local health care leaders and communities.

[Minimal security risks, political viability] Experts suggested that the only way an HRB could operate successfully would be if it assembled all patients' data from all providers in a region. This was believed to be possible only if patients were automatically enrolled, which could pose a substantial risk of backlash and therefore lack political viability. A large repository of data in itself creates risk of a security breach. To protect security, one proposed approach involved storing each patient's record with separate encryption keys (Yasnoff and Shortliffe, 2014).

[Feasibility and sustainability] Some experts were skeptical that the large up-front investment needed to prove the business model would be feasible. One attempt to start an HRB, in Phoenix, Arizona, failed quickly due to low enrollment and lack of revenue (Yasnoff and Shortliffe, 2014). Few patients wanted to pay for the HRB, and providers (whose referrals were believed to be the best method for recruiting patients) did not want to ask patients to pay for it. Making a basic account free and charging for optional services could improve uptake.

Solution 9: Having Patients Manually Verify Matches

In the interviews undertaken for this project, some experts discussed the option of allowing patients to manually verify matches that occurred, through their patient portal or a software application available in the clinic (e.g., kiosk, tablet). Privacy concerns and regulations, such as HIPAA, prevent patients from being shown candidate matching records that may belong to other people. Therefore, identifying false negatives is more challenging using this method. Still, such an approach could be used to allow patients to verify and confirm matches after they do occur, which would allow them to identify the (hopefully rare) false positives, and also to flag cases when expected matches do not occur, such as for previous visits to different providers.

Evaluation of Solution 9

[Improvement in record matching if widely implemented] If patients used this solution to verify matches that occurred, false positives would be identified, but they are relatively rare and most of the time patients would simply confirm correct matches, which some may find valuable but others may find tedious. False negatives are much more common but would require patients to proactively flag them, and it is unknown how doing so would help providers locate the missing records. (This solution may therefore need to be combined with other solutions, such as Solution 10 below.)

[Likelihood of adoption by patients] Although patients arguably have the greatest stake in record matching, this solution would require additional work from them, with questionable perceived benefit. Therefore, this solution may improve record matching only marginally, and few patients may bother to verify matches unless the process is made very easy for them.

[Likelihood of adoption by providers] Providers may be concerned about offering this capability to patients if it resulted in additional interactions to explain how it works or if patients made mistakes in determining if matches were correct. However, if such functionality is available in patient portals, it may provide an opportunity to educate patients about the importance of record matching and the severity of the problems that currently occur due to record matching failures. Solutions that involve kiosks or tablets may reduce the burden on front desk staff but at additional cost.

Solution 10: Having Patients Supply Record Location Information

Even if patients do not have copies of their actual health records, their knowledge of where their previous records are located could be useful in record matching. For example, if patients are able to specify the geographical regions or provider systems in which they have previously received care, matching engines (or front desk staff) could use that information to find the correct records, and disregard others, thereby improving match rates. This method may be most effective in combination with others, such as when querying for records as part of consumer-directed exchange or when signing up for an HRB. CommonWell Health Alliance has implemented and tested this approach, wherein front desk staff view a list of candidate matching records and verbally ask patients to confirm which records are theirs by asking about their previous health care providers and appointment times.

Experts suggested solutions that have a similar workflow but with different kinds of questions asked of patients. For example, the patient might be asked about different kinds of information, such as their past medical history, which could help identify the correct medical records; alternatively, knowledge-based questions that could help link records to known identifying information from external sources, such as credit bureaus, could be incorporated into matching.

Evaluation of Solution 10

[Improvement in record matching if widely implemented] To the extent that patients know the correct answers to the questions they are asked, patient-supplied information may help improve record match rates considerably if widely used. When implemented as part of consumer-directed exchange, this solution has the potential to help find patients' records if they are allowed to search multiple regions or HINs to locate them.

[Likelihood of adoption by patient, likelihood of adoption by providers] Implementing this solution would require additional work for patients and providers. CommonWell's experience is instructive: When front desk staff asked patients to help them identify which records were theirs based on location, patients were confused and front desk staff had difficulty explaining the purpose of the questions because most patients assumed the provider already had their records. In addition, some patients may not remember their previous care locations reliably when asked. Kiosks or tablets may streamline the process but would entail additional expenses for providers.

Chapter Summary and Analysis

Our work identified a wide range of possible patient-empowered solutions to improve record matching (some more empowering than others). We were able to find more extensive detail for some of the proposed solutions, whereas information on others consisted of overarching ideas or concepts that did not explain how the solutions would work, or had not been fully developed, piloted, or implemented. Solutions also ranged widely in terms of certain details such as the data types used for record matching and the workflow changes that would be required of providers. Although these ten proposed solutions are not mutually exclusive—and in fact they may have promising synergies—we were tasked to select one solution (or a cluster of solutions) that, based on available data and our analysis, holds promise as a patient-empowered approach to improve record matching.

Despite limitations in existing evidence, our analysis shows that the appeal of some of the solutions is obvious, and yet their drawbacks are evident, too. For example, biometrics-based approaches are surely convenient, but at the same time, fingerprints cannot be changed if compromised. Consumer-mediated exchange solutions are ideal for promoting patient control, but they have questionable return on investment for providers and thus lack the business case necessary for widespread adoption. Our analysis suggests that a reasonable argument could be made for almost all of the potential solutions. In fact, for many solutions, experts claimed the benefits exceeded the costs. (RAND also came to that conclusion about a unique patient identifier in previous work [Hillestad, Bigelow, Chaudry, et al., 2008].)

To select a promising solution, we sought the opinions of experts and weighed the evidence with the assistance of our expert panel. Experts emphasized the limitations and challenges associated with all of the potential solutions, and we did not identify a "silver bullet" solution. Key challenges to all solutions are engaging patients, who likely do not recognize existing

problems with record matching, and engaging providers because doing so will likely require them to make major changes in staff workflows, core business and administrative processes, and technology—not an easy thing for an organization to commit to, especially if there is uncertainty as to whether it will succeed and catch on among other organizations. These challenges may in part explain the failures of some previous attempts at consumer-mediated exchange. Although consumer-mediated exchange may be the ideal from the point of view of patient-empowerment, previous attempts to implement that solution suggest that the "perfect" may be the enemy of the good, at least in the near term. The same critique may be made of blockchain-based approaches to consumer-mediated exchange solutions promoted recently in white papers (see Appendix F).

As a result of our analysis and consultation with Pew and our experts, we selected an approach to patient-empowered record matching that combines several of the record matching solutions. Specifically, as elaborated in the next chapter, ours is a three-stage solution that combines elements of expanding the use of existing government-issued identifiers (Solution 3), verifying identity information (Solution 6), consumer-directed exchange (Solution 7), and an identifier-based solution involving HINs, which was articulated in the context of HRBs (Solution 8).

The ultimate success of any potential solution will depend on a number of factors, not the least of which is timing. The landscape of health care and technology (for patients and providers) is changing rapidly, and what may seem to be the best approach today may be viewed differently in a few short years. For example, changing public opinion on privacy due to recent breaches and mis-uses of data may result in legal action to protect privacy, which may affect biometric-based approaches. We have attempted to select a solution that would be robust vis-à-vis such potential changes and provide a foundation for future advances that may enable greater improvements in record matching.

6. Advancing a Mobile Phone Solution with App-Based Functionality in Three Stages

In our assessment of potential patient-empowered solutions to record matching problems, we found several promising approaches but also barriers to, and a high degree of uncertainty about, their success. Although some experts claimed that the benefits outweighed the costs for several specific solutions, the literature and discussion with experts revealed substantial challenges for all potential solutions.

After considering the information and arguments presented in the previous chapters, we developed the outlines of a three-stage solution that synthesizes several components of the other solutions. In particular, we propose a system in which patients are able to "verify" their identity information, starting with mobile phone numbers, to their providers, and then, building on the concept of verified attributes, use smartphone app functionalities for bidirectional communication with their providers to exchange identity and health care information. Patients would use these apps to check in to appointments and send providers additional identity information (e.g., name, address, government-issued ID), which may be verified through an app-supported identity-proofing process, thereby simplifying the front desk check-in process for both patients and providers and improving the quality of data that health care providers currently use for record matching. Apps would in turn receive patient health data, allowing patients to accumulate their data and further facilitate record aggregation. This aggregation of data may have the potential in the future to be exchanged directly with providers, and thus reduce the need for record matching based on identity information and help to realize the vision of a personally controlled health record (Szolovits et al., 1994). Therefore, rather than choosing between current provider-to-provider exchange methods and long-proposed consumer-mediated exchange, we propose a solution that advances both at the same time—while acknowledging that widespread use of consumer-mediated exchange will likely require additional effort beyond our proposed solution.

We present this proposed solution in the form of three stages, describing the sequence of development and implementation that we would expect to see. We recognize, however, that development could advance in all stages simultaneously, or that implementation could occur in a somewhat different sequence, or both. In the first stage, we propose the concept of "verified" patient identity information. For example, a patient's mobile phone number can be verified at a specified level using a one-time passcode. This will require the development of technical specifications for metadata,[1] which indicate the quality of identity information and will help

[1] In this case, the metadata would describe the level of verification of identity data. High levels of verification would suggest higher levels of data quality and utility in matching engines.

improve the accuracy of matching engines. In the second stage, we describe the basic functionality of a patient-controlled smartphone app that would transfer identity information to providers and, in turn, facilitate the transfer of patient health data into the app to improve the value proposition to increase adoption. In the third stage, we describe more advanced functionality that may improve the value proposition for patients and providers—and encourage uptake—and build upon current efforts of HINs as well as the ONC's plans to promulgate a TEFCA. Lastly, we discuss governance considerations for advancing this work and protecting patient privacy.

Table 6.1. Three-Stage Solution to Patient Record Matching

Stage 1: Add Verified Patient Identity Information	Stage 2: Add Basic App Functionality	Stage 3: Add Advanced App Functionality
• Technical specifications for verified attributes are established • Workflows and best practices to verify attributes starting with mobile phone numbers are developed • Workflows and best practices to facilitate patient sign-up for existing patient portals are developed	• Technical specifications define APIs that enable bidirectional communication between a patient app and provider • Patient app can send identity information (including attributes verified by app) • App can return provider contact info and instructions to sign up for patient portal • Governance ensures apps are trusted	• Apps can facilitate identity-proofing to increase number of verified fields • Credentials from app can be used to log in to patient portals, facilitating health data aggregation in app • Validated insurance information can be stored in app and transferred to provider with other identity attributes • Unique identifiers issued by HINs can be stored in app and transferred to provider with other identity attributes

Stage 1: Verified Patient Identity Information

As described in Solution 6 (Chapter Five), when health care providers currently receive identity information, the information does not include any assessment of data quality, and so existing matching engines are limited by their inability to easily distinguish highly reliable attributes from poor-quality ones. For example, a matching engine today cannot distinguish between an up-to-date address or phone number and one that was recorded decades ago and never updated. If matching engines were able to determine data quality in a standardized fashion, providers would likely be able to improve the accuracy of their matching algorithms by giving greater weight to the most reliable data elements and less weight to the others. Therefore, we introduce the concept of a "verified" patient identity attribute, the reliability of which would be indicated using metadata. Ultimately, this concept may apply to any patient identity data element used for record matching, but to begin with, we will focus on mobile phone numbers because methods for verifying them, which utilize existing telephone infrastructure (e.g., sending a one-time passcode), are widely used, a large majority of patients possess them, and mobile phone

numbers are unique and change infrequently, although the rate of turnover in phones and phone numbers may be high among the homeless population (Rhoades et al., 2017).

To facilitate widespread adoption, verification of patient attributes would likely require the development of an open-source technical specification that is implemented by all software systems that capture patient identity information. The specifications would need to include syntax of the data fields (format) as well as semantics (workflow steps required to justify a level of verification). Verification fields may include the details of verification such as mobile phone number used, the date, the verification level, the verifying party, and an optional digital signature that would provide greater assurance that the field was verified. See Table 6.2 for an example.

Table 6.2. Examples of Data That Would Fill Verification Fields

Field	Data
Mobile phone number	555-555-5555
Date	MM/DD/YYYY
Verification level	Level 3
Verifying party	Dr. Alice's Clinic
Digital signature (optional)	None

Various levels of verification will need to be defined as part of the technical specifications, which may be consistent with NIST standards for authentication (NIST, 2018). (However, because the purpose here is record matching rather than authentication, the definition of the levels may need to be different, depending on the outcomes of pilot testing for feasibility.) For example, at patient check-in, the front desk staff may ask for the patient's mobile phone number and type it into the provider's registration software. At that point a text message can be automatically sent to the patient's mobile phone asking the patient to respond with a text message containing the letter "c" (for "confirm"). If the patient sends confirmation, her mobile phone number's level of verification field is set to Level 1. For higher levels of verification, the text message might ask the patient to respond with her year of birth, or it may contain a six-digit one-time passcode that the patient would be expected to show the front desk staff, who would then type it into the registration software. This higher level of verification would be an increased burden for the front desk. (That burden could be mitigated if patients used a tablet or kiosk to perform this verification. In that case the patient would check in using the tablet or kiosk and enter the one-time passcode directly into the tablet or kiosk.) Doing so would result in higher levels of verification recorded in the mobile phone number's metadata. The specific workflow and user interface details could be informed by pilot testing and experimentation, and ultimately will be up to the software implementer, but the fields would require standardized definitions. Vignette 5 illustrates this workflow.

Vignette 5: Verified Patient Identify Information

Patient Jane goes to Dr. Bob's office for a routine visit. A front desk staff member finds Jane in the patient registration system, which sends a one-time passcode to Jane's mobile phone number on file. The staff member asks Jane for the passcode, and then enters it into the registration system, which labels the phone number as verified. If Jane does not receive the text message, the front desk staff checks to make sure they have the correct mobile phone number. When Jane checks in at subsequent providers, her phone number is also verified in the same way, and so when the providers exchange Jane's records, the phone number is used by the matching engine as a highly weighted attribute.

Currently, when providers transfer their registration information into new systems (e.g., for upgrades), errors are common because ad hoc, manual processes are often used (e.g., downloading the data to a spreadsheet file and uploading it to the new system). Therefore, to ensure the integrity of the verified fields, rules governing the transfer of validated identity attributes would be required. Verified identity attributes would likely no longer be considered verified if data is transferred using ad hoc processes; in those cases patients would have to verify their attributes again.

To improve the provider value proposition, best practices may be established in which the verified phone number (or email address) facilitates patient sign-up for a provider's patient portal by sending a text message with a link to the provider's patient portal sign-up instructions. This would help providers meet federal requirements that promote patient engagement and data access. Providers may find additional benefits to verifying fields, such as ensuring a patient's mobile phone number is correct to make it easier to get in contact with them.

Stage 2: Basic App Capabilities

Our second stage proposes to create a system in which an app on patients' smartphones would establish bidirectional communication directly with their health care providers' registration systems. When a patient checks in at the front desk, the app would send patient identity information from the patient to the health care provider, thereby simplifying some aspects of the "clipboard" process. (Automating the entire clipboard process is a laudable but complex goal, given the variability of the information collected by different providers and the perceived utility of requiring patients to recall their health history.) The provider registration system would, in return, send to the patient the provider's contact information as well as instructions for how to sign up for a patient portal and link it to the app. Developing this functionality would require new open-source technical specifications to define the APIs for

bidirectional communication. To encourage provider and patient adoption, there would need to be a mechanism to ensure that both parties could be trusted (see the "Leadership and Governance Considerations" section below for details). The workflow for this may follow the example in Vignette 6.

Vignette 6: Basic App Workflow

Patient Jane installs an app and enters her identity information, including name, date of birth, address, gender, home phone number, mobile phone number, and insurance information. Subsequently, when Jane comes to Dr. Bob's office as a new patient, she opens her smartphone app and uses it to generate a *quick response* (QR) code, which the front office desk would scan using a commercial off-the-shelf scanner. Dr. Bob's patient registration software would use the information in the QR code to pull Jane's identity information from the app.

Other workflows are possible, such as using *near-field communication* (NFC), which would require the patient to tap her phone on a terminal. In return, the time and date of the check-in and Dr. Bob's contact information would be recorded in the app, so that Jane would have access to an ongoing history of her previous appointments. Jane would also receive instructions for how she could register and sign into Dr. Bob's patient portal and then link the portal to her app so that her health data would be automatically aggregated.

Stage 3: Advanced App Capabilities

To further improve record matching and the value proposition of a smartphone app for both patients and health care providers, we describe four examples of advanced functionalities that could be developed for the smartphone app: verify additional patient identity attributes through identity-proofing; provide credentials that allow patients to register and sign in to their patient portal—without needing to manage login credentials for each portal—and aggregate health data in the app; transfer verified insurance information (e.g., group number and ID number) to providers; and obtain unique identifiers issued and managed by HINs. These functionalities are meant to serve as examples for further investigation. Some may prove more feasible than others. Additional advanced functionality, such as further automating paper-based and manual processes for capturing basic health history information, should also be considered.

In the first advanced feature, an app would facilitate identity-proofing, thereby verifying several of the patient's attributes, such as name, date of birth, address, and driver's license number. Recent standards promoted by NIST for levels of identity-proofing may be utilized.

For example, *identity assurance level* (IAL) 2 may allow for patients to identity-proof remotely, by taking a picture of their driver's license with their smartphone along with a live picture of themselves, among other requirements. Higher levels of assurance require in-person verification of identity. (The appropriate level of assurance would need to be determined through a stakeholder consensus process.) Once a patient downloads an app and uses it to identity-proof herself, her verified identity information would be transferred when she checks in at her provider's office with the app, and then the verified attributes could be used in matching engines when her medical records are exchanged by her provider with another health care provider.

The second advanced feature, app login credentials, builds on the first. After a patient is identity-proofed, she would be given login credentials (e.g., username and password, or a FIDO[2] authentication method) that she can use from that point forward to sign into the patient portal(s) of any providers for whom she has used the app to check in. This helps the patient avoid the need to register for and keep track of multiple login credentials, thereby facilitating the use of multiple provider patient portals and access to her health data. Insurance companies may also allow patients to use their app credentials to log in to health insurance portals (such as those that allow patients to track provider claims, insurance payments, and explanation of benefits).

The third advanced feature is consistent with a previous effort made by the WEDI to create a Virtual Clipboard to facilitate the transfer of insurance information (WEDI, 2016). This feature would allow patients to store proof of insurance information that is verified by insurance companies in an app and transfer it to their health care providers, further simplifying the clipboard process for patients and providers.

For the fourth advanced feature, we borrow the concept of a unique identifier issued by an HRB (Chapter Five, Solution 8), but foresee that unique identifier numbers being issued by a *qualified health information network* (QHIN), as defined under the ONC's recently released draft TEFCA, which outlines methods and principles for the exchange of health data among QHINs (ONC, 2018a, 2018b). Although still in draft form, this framework has the potential to change the landscape of data exchange, in terms of structure (by defining a new *recognized coordinating entity* [RCE]) and process (by defining requirements for QHINs and for individuals to participate). TEFCA opens up the possibility that an identifier issued and maintained by one QHIN could be used to uniquely identify patients when they receive care from a provider who is a member of a different QHIN. See Vignette 7 for an example.

[2] FIDO standards aim to replace the requirement of users to maintain multiple username and passwords with more user-friendly authentication methods that rely on public key cryptography, hardware tokens, and local biometrics. These standards would facilitate patient access to patient portals via their smartphones. FIDO standards are expected to become universally adopted by popular smartphone operating systems and web browsers.

Vignette 7: Advanced App Capabilities

Patient Jane checks into Dr. Bob's office using a trusted app in which she has been identity-proofed. Dr. Bob's registration software then makes Jane's identity information available to the QHIN he participates in, so queries from other providers are able to locate Jane's records. The QHIN would then return a unique QHIN ID for Jane. Dr. Bob's registration software would save the QHIN ID in Jane's record and then send it to Jane's app as a data element verified by the QHIN. When Jane checks in to subsequent providers, the QHIN ID would be transferred to her providers along with her other verified identity attributes, and the providers would use it in queries and messages to uniquely identify her.

Although many HINs might be reluctant at first to share identifiers externally because of concerns about the effort and responsibility required to manage identifiers, some existing HINs are beginning to share their identifiers with health care providers for the purpose of helping providers create consistent links between their records and the HIN's records, and to ensure demographic information is consistent (e.g., Michigan Health Information Network's "Common Key"). Sharing identifiers with patients may be a logical next step. This additional attribute would improve matching for cases in which a patient's other attributes (e.g., mobile phone number, driver's license number) have changed, and may reduce the need to share as much other patient identity information.

Leadership and Governance Considerations

The solution we describe above contains multiple components involving diverse stakeholders, the details of which will likely become apparent only after some initial technical development and pilot testing for feasibility. We provide some preliminary considerations as to the leadership and governance needed to ensure that this work progresses systematically—from pilot testing through ongoing operation.

It would be beneficial if there was one organization to provide leadership, support, and tracking of pilot tests and evaluation, as well as to convene key stakeholders to build consensus where consensus is needed. This organization could be the TEFCA RCE or another neutral third party. Its mission would include improving record matching. This organization would not need to manage all aspects of record matching—for example, it may not need to be involved in standards development processes because organizations that can serve that role already exist—and its role will likely evolve over time. Although it is unknown if this organization would be most helpful by serving as a convener or by taking a more active role, it should begin by

focusing on pilots to develop and refine technical specifications and best practices, and then consider governance needed to ensure apps are trusted, including the possibility of certifying them. Apps will need to be trusted in two ways: (1) Providers and patients will need to trust that apps will be implemented securely and function without major technical issues; and (2) patients will need to trust that apps adequately protect patient privacy and do not share data against their wishes. One major incident with one app in either regard might have a devastating effect for all apps.

There is a range of governance options to ensure apps are trusted in these regards. At one extreme, providers may be on their own to choose which app vendors to support. This approach would not require a centralized process but may be more burdensome to providers who would need to evaluate various apps and determine which they will support, if any.

At the other extreme, a trusted third-party organization could certify apps to give providers and patients extra assurance that the app meets specific criteria. Vendors may be certified based on reliably adhering to technical specifications, security standards, and/or consensus-based policies for informed consent and data sharing. To protect patient privacy, apps may also be certified for using privacy policies and end-user licensing agreements that meet specific standards. This arrangement could create a burdensome approval process that might delay adoption and increase overall costs to the app developers (which would likely be passed downstream to the paying customer).

A middle ground is possible, however. For example, a governing organization may issue a set of principles that an app vendor would attest to for each product. This is the approach that a new organization called Xcertia, founded by the American Medical Association and other health care organizations, is taking to encourage best practices related to security and usability among mobile health apps (“Xcertia mHealth App Guidelines,” 2017). The CARIN Alliance has also developed a set of guidelines for applications exchanging data outside of HIPAA (CARIN Alliance, 2018).

7. Assessment of Selected Solution Using Evaluation Criteria

To further investigate the strengths and weaknesses of our proposed approach, we consider the components of our three-stage solution in light of our evaluation criteria.

Evaluation of Three-Stage Solution

Criterion 1: Improvement in Record Matching if Widely Implemented

If used widely, verified patient identity attributes would improve record matching by eliminating clerical errors and improving the quality of data used by provider matching engines. Mobile phone numbers alone would make a substantial improvement in match rates, and use of other verified attributes would make further improvements. If universally adopted and used consistently within secure apps, the use of QHIN IDs would increase match rates to near perfect because they would function as de facto universal identifiers.

Criterion 2: Patient Control

Patients would have control over which identity attributes they validate through providers, and the proposed smartphone apps would likely allow patients to choose which identity attributes to share with providers. Patients could also refrain from participating altogether. Our proposed solution does not provide a mechanism for granular data segmentation and access control. However, in the longer term, the solution may enable greater options for patient control over matching and exchange by facilitating aggregation of data in a patient-controlled app. Therefore, our solution strikes a balance by improving match rates using current provider-to-provider exchange mechanisms, in which granular control is not possible, while laying a foundation for consumer-mediated exchange, in which granular control may be possible.

There is always the risk that identity and medical data stored in a smartphone app could be used by the app vendor for purposes contrary to a patient's preferences or interests because app vendors are not "covered entities" under HIPAA. The FTC and ONC have worked together to provide guidance to mobile health app developers on their responsibilities to consumers as well as the various federal laws that may apply ("Mobile Health App Developers: FTC Best Practices," 2016). It is unknown if these federal protections would be sufficient to protect patient privacy if massive amounts of data were stored in smartphone apps under patient control. Although a comprehensive privacy threat analysis is beyond the scope of this project, in the wake of recent events in which Facebook data were shared and used for political purposes against user preferences, new legislation may be required to address privacy and security issues. But absent the passage of more protective legislation, a governing organization could, at a minimum, serve the role of reviewing and certifying app vendor privacy policies to determine

if those policies adequately focus on the privacy and security of uploaded data and on patient preferences (see Chapter Six, "Leadership and Governance Considerations" section).

Criterion 3: Likelihood of Adoption by Patients

Any patient with a mobile phone would likely encounter minimal barriers to verifying his or her phone number (Stage 1). For Stage 2 and 3, although a public information campaign that educates patients about the benefits of improved record matching may help, improved matching may be insufficient motivation for patients to purchase or use a smartphone app. However, the approach we have outlined may provide the following additional value for patients:

- eliminate the need to maintain multiple login credentials, essentially creating a master patient portal login credential;
- simplify "clipboard" paperwork—patients would no longer need to fill out identity information or proof of insurance information; although clipboard contents, such as medical history, may be more challenging to automate, apps may store commonly used clipboard information (e.g., family history, dates of surgeries) that is sometimes difficult to remember;
- allow patients to keep an ongoing log of their health care appointments and their provider contact information; and
- facilitate patient's ability to aggregate their health data and use it for other purposes.

We expect that app vendors will develop innovative functionality to compete in the marketplace by improving the value proposition of their particular app for prospective consumers. These more advanced functionalities may include: allowing patients to request and schedule appointments with providers; providing calendar functionality that tracks their appointments and sends reminders; subscribing to relevant newly published research studies and news articles; receiving invitations to participate in new research studies; sharing patient-generated health data (including patient-reported outcomes data and device data such as from fitness trackers and glucose monitors) with their providers or researchers; sharing data with disease-specific monitoring programs; and tracking payment and billing interactions with insurance companies.

At first, the types of patients most likely to use an app may be those who are early adopters of technology, those who are more engaged in their health care, and those with multiple chronic conditions who visit multiple providers. Engaging patients with multiple chronic conditions could be a significant feat, because they are the patients who incur the lion's share of health care costs and would likely benefit the most from such an app. Patient adoption will be dependent on provider adoption: If patients can use the app with all of their providers, they will be more likely to use it. Providers may also play a critical role in patient adoption by encouraging uptake among patients. (See sections below on provider and vendor factors.)

Barriers to patient adoption exist. Verification requires an extra step for patients in all cases, and some patients may view identity-proofing (even if done remotely) as a barrier. In fact, some

patients cannot be identity-proofed easily, or do not have government-issued IDs. Also, not all patients will have smartphones, although currently adoption is greater than 80 percent and is growing, especially among elderly and low-income individuals (Anderson, 2017; Anderson and Perrin, 2017; Pew Research Center, 2018). Even those without smartphones often have parents (in the case of minors) or adult children or caregivers (in the case of disabled adults or the elderly) who own smartphones and may be willing to use an app for these purposes. But even for patients who have smartphones, not all will be able or willing to use them for this purpose because of differences in familiarity with, and challenges in using, apps. Therefore, as with all software, usability will be critical to user engagement.

Criterion 4: Likelihood of Adoption by Providers

Health care providers may be the most important and yet most challenging type of stakeholder to engage in every stage of our proposed solution. Providers would need to add new check-in workflows or change their existing processes. Previous attempts to get providers to change their workflow to improve record matching (i.e., CommonWell Health Alliance's attempts to collect government-issued ID numbers for record matching) struggled to gain widespread adoption, and some of our experts suggested that any attempt to change any aspect of provider workflow would meet with either inertia or steep resistance. However, our proposed solution would have several potential benefits for providers:

- It would establish specifications and best practices for collecting verified patient identity attributes that have value to providers (e.g., mobile phone numbers to ensure they know how to contact patients).
- It would simplify the check-in process in a way that reduces the burden on front desk staff while increasing data quality.
- It would provide additional validation that patients are who they say they are (although the potential for fraud still exists if patients were to use someone else's smartphone).
- It may improve their ability to capture proof of insurance information in real time.
- It would facilitate patient registration, sign-in, and use of provider patient portals.
- It may enable providers to receive credit under the CMS Quality Payment Program (QPP) for one or more patient-centered measures (e.g., provide patient access, patient-specific education, patient-generated health data).
- It may facilitate repurposing of existing hardware (an estimated 43 percent of credit card payment terminals were enabled with NFC in 2015 (Boden, 2017) but even if new hardware is required, QR code scanners are inexpensive.

Yet, some providers may be reluctant to adopt such a solution because:

- Any change in workflow, particularly within larger health systems, would require strong support from leadership.
- Providers in competitive markets might support or offer competing apps and may be reluctant to participate in a system that allows other apps to be used to log in to their patient portals (but this may be considered "data blocking" and therefore illegal).

- EHRs and record matching engines may need to be updated to incorporate verified fields.
- Front desk staff may be reluctant to learn a new system and be likely to abandon the solution if there were any technical issues.
- Providers may need to educate patients to achieve high adoption, potentially creating more work for their staff.

As they would for patients, app vendors will hopefully develop additional innovative functionality to increase the value proposition for providers. Experts suggested that smartphone apps may help providers track patients in other settings to promote accountable care (e.g., notifications of ED visits, hospital admissions, missed referral appointments) by allowing providers to "subscribe" to notifications of app-supported check-ins with other health care providers.

The pace of adoption is hard to predict, and there will likely be providers who will not change processes or support this type of app. However, if even a small number of large, well-respected, high-profile health systems (e.g., Kaiser Permanente, Intermountain) adopted components of this solution, other health care providers would likely follow because of the perceived need to keep up with industry standards. If major payers such as CMS or the Blue Cross and Blue Shield Association endorsed adoption, large numbers of providers would likely follow. And if this solution is shown to significantly reduce matching errors and/or improve coordination of care, many providers will adopt it voluntarily. Some, however, may adopt the solution only if required by policymakers.

Criterion 5: Likelihood of Adoption by Vendors

Patient registration software and EHR vendors would need to implement technical specifications for incorporating identity metadata for verified attributes and support APIs to allow bidirectional communication with apps. Matching engines would also need to be updated to support these attributes. Patient portals would need to allow patients to use app-based login credentials. Some vendors may be willing to support these changes, especially if demanded by providers, but others may support them only if incentivized or required by policy.

Criterion 6: Feasibility

Development of technical specifications and pilot testing prototypes to establish proof of concept and demonstrate feasibility would likely require only modest resources. However, as with many technical specifications, there is a risk that vendors may interpret them differently, which would reduce their utility when, for example, verified attributes are shared across vendors. Pilot testing an array of different vendor interpretations of the technical specifications may help inform their refinement and identify ambiguity. Feasibility of ongoing operation is difficult to assess without further development and pilot testing of the components of the solution.

Criterion 7: Minimal Security Risks

The addition of verified attributes—stored by providers—may make provider information systems a more attractive target for hackers. Additionally, smartphone apps that gather health data would introduce two types of risk. First, apps would contain high-value, private information—including demographics, ID numbers, and patient health data—and second, they would therefore be a target for hackers to steal data (or to use the app to steal data from provider-based EHRs). Any PHR linked to an EHR also would have these concerns. Although a comprehensive security threat analysis is beyond the scope of this project, we consider a few security-related situations and how an app might address them:

- Patient loses her phone: If the phone is locked, security risks are minimal. Even if the phone is not locked, the app will likely require either a password or biometric to log in.
- Patient's app account is hacked: As with any hack, the contents stored in the app—which will include patient's identity information and medical records—would be accessible to hackers and could be sold or used for blackmail or ransom. The data could also be used for fraud, but methods similar to mobile payment applications could be used to mitigate against the threat of stolen proof of insurance information. Also, some apps may allow providers to view a picture of the patient to further verify their identity.
- Phishing attacks: As with any app that contains valuable data, patients may receive phishing emails in an attempt to get them to surrender their password and account information. The requirement to have a verified mobile phone number in order to access the app may reduce this risk.

Somewhat mitigating these security concerns, according to experts with whom we spoke, is that the apps would likely be covered under the FTC's breach notification rules for PHRs, which was a provision of the HITECH Act of 2009.[1] In addition, there are breach notification laws in all 50 states (Skadden et al., 2018). However, it is unknown if these laws are sufficient to ensure that app vendors invest in appropriate security safeguards.

Second, apps could be commandeered and used to compromise provider information systems. A hacker could develop a fake app that mimics a trusted app and use it to try to check in to a health care provider (in person or remotely) and request medical record information. Preventing this would require that EHR vendors send records only to trusted apps, so the list of such apps would need to be maintained and updated.

Criterion 8: Sustainability (Financial and Operational)

Use of validated mobile phone numbers, once specifications and workflow processes are established, should be sustainable and require no ongoing costs. App vendors will be expected

[1] A PHR is defined under the regulation as an electronic record of "identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual." (AHIMA e-HIM Personal Health Record Work Group, 2005).

to establish a business model to cover the costs of app development. We expect most to offer a basic version of the service free to patients and to charge the patients (or other parties) for advanced functionality. We expect that employers or public or private payers (such as commercial insurers, CMS, Department of Defense, Veterans Administration, Washington Health Care Authority, Massachusetts Group Insurance Commission, etc.) might be willing to pay for advanced features as a part of a health benefits or wellness package. Other business models may be possible.

Criterion 9: Political Viability

The initial development and pilot testing of technical specifications and workflows for implementing verified attributes and basic app functionality likely would not require political support or consensus. However, for apps to be trusted, a stakeholder consensus process will likely be critical. The development of advanced functionality in particular (e.g., processes for identity-proofing, credentials for portal sign-in, QHIN-ID workflow rules) would likely require stakeholder consensus to establish basic parameters. Enabling legislation or federal agency support would not be required to develop the solutions but may ultimately help achieve a "tipping point" of adoption among providers who are already dealing with a host of externally generated priorities.

Criterion 10: Potential to Foster New Uses of Matched Data

By allowing patients both to log in to each provider's patient portal using one set of credentials and to link their smartphone app to their patient portal at the time of check-in, our proposed approach has the potential to accelerate patient access to their own health information. This in turn would allow patients to use the data in new and innovative ways. (See Criterion 3 above.)

Criterion 11: Low Potential for Unintended Negative Consequences

At this early stage it is difficult to anticipate "unintended" consequences, and one would hope that many of the potentially negative consequences would be identified and resolved through pilot testing and iterative development. However, based on our discussion with experts, we can anticipate a few issues that may arise.

As patients begin to the use the app for the first time, there may be the potential to increase local record duplicates (such as when an identity-proofed patient is matched with local identity data at check-in, and the front desk staff does not make the connection). Also, if technical issues with an app arise at check-in, it is likely that patients and the front desk staff will abandon the app. Finally, if more patients have easier access to their medical records, patients may ask their physicians additional questions during visits about what the data mean, increasing provider workload. However, that latter concern has been shown to be minimal when patients had access to clinical notes (Bell, Delbanco, and Walker, 2017).

Chapter Summary and Analysis

As we have described in this chapter, our analysis of the strengths and weaknesses of the three-stage solution that we have proposed, based on our review criteria, indicate that it is not a perfect solution or "silver bullet," but it does have a decent chance of a high and incrementally increasing adoption rate, which in turn would result in a consequent reduction in matching errors as validated identity information comes into play. More cannot be said without further development of the model and pilot testing under real world circumstances with a meaningful evaluation. We now turn to our conclusions and recommendations for next steps in Chapter Eight.

8. Conclusions and Next Steps

In this work, we identified ten potential solutions to record matching that involve a more expanded role for the patient. Some of our experts expressed skepticism that any new role for the patient was feasible, because, they said, patients expect the health care system to solve this problem without any effort on their part, or because of the challenges observed in making even small changes to provider workflows. Despite these challenges, our findings suggest that there are several potentially promising patient-empowered solutions that heretofore have not been the focus of systematic development or pilot testing. Although all solutions require further development and testing to fully assess their potential, our analysis suggests that there are a number of other options that present opportunities to make progress. Further, by proposing our three-stage solution, we have selected an option that does not require federal action to advance; rather, it can be developed iteratively and implemented incrementally with the potential that new functionality can be added over time.

Although we did not identify a "silver bullet" or achieve consensus on a single most promising solution, the three-stage approach we recommend, based on our analysis of options, has the potential to directly improve provider-to-provider record matching by increasing the type and quality of identity information used by matching engines (and, in particular, explicitly capturing the degree of data quality) beginning with the use of verified mobile phone numbers and extending to more data elements via new capabilities of smartphone apps. Our proposed solution would also help accelerate health data aggregation under the control of patients, thereby fostering consumer-mediated data exchange in the longer term.

We make five recommendations. The first three advance this three-stage solution, which we believe will spur broad-based adoption of a low-cost, feasible, and sustainable solution by patients and providers. The final two recommendations would support a range of record matching solutions. To ensure that the development work for the first three recommendations proceeds expeditiously and is rigorously evaluated and that the results are disseminated, funding would likely be required to pay application designers, software developers, evaluators, and possibly other participants until the technology and best practices are established. To achieve widespread adoption, the technical specifications and best practices resulting from the development efforts we recommend would need to be widely and freely available, and so funding for them would most likely need to come from stakeholders dedicated to improving record matching, rather than those who expect to make a profit.

Recommendations

Recommendation 1. Develop technical specifications for verified data fields, develop best practices that allow health care providers to verify mobile phone numbers, and iteratively pilot test and refine the specifications and best practices to maximize feasibility and usability.

To advance Stage 1 (the development of verified patient identity attributes), technical specifications and best practices for implementing them would be needed. This work should be conducted by a team of application designers and software developers and pilot tested with at least two participating provider organizations that share patients and use a matching engine. Although the workflows may seem simple, previous experience has shown that even small changes to front desk responsibilities are challenging and require careful design and testing. As part of development and pilot testing, vendors will need to modify their patient registration software to accommodate new data fields, and provider matching engines will similarly need to be updated. A variety of provider workflows (at different levels of verification) should be tested and iteratively refined for feasibility and usability, from both the patients' and the front desk staff's perspectives. This testing may reveal important tradeoffs. For example, workflows in which patients are asked to respond to a text message to confirm their mobile phone number may be simple to implement from a provider perspective, but patients may be confused by it unless the front desk staff tell them to expect it. Rapid-cycle development and evaluation of implementation using a small number of health care providers will likely quickly reveal the major barriers to this approach as well as the methods for overcoming them.

As initial feasibility is demonstrated, pilot testing with an expanded group of providers in a diversity of settings, such as emergency room, hospital, ambulatory clinic, safety net clinic, will allow for further refinement. Ultimately, these new specifications should be introduced into existing technical standards, such as the *Fast Health Interoperability Resources* ("FHIR Release 3 (STU)," 2017), the *Consolidated Clinical Document Architecture* (CCDA) (HIMSS Interoperability & Standards Practices Task Force, 2014), *HL7* v2 Messaging ("HL7 Version 2 Product Suite," 2018), and the *Argonaut profiles* ("HL7 FHIR Argonaut Project," 2018).

Recommendation 2. Develop APIs and best practices for establishing bidirectional communication between a smartphone app and health care provider registration systems at the point of care, and iteratively pilot test and refine them.

To advance Stage 2 (basic app functionality that facilitates bidirectional communication between patients and providers), development of prototype APIs and best practices for implementing them are needed. As with Stage 1, this development work should be conducted by a team of application designers and software developers and pilot tested with at least two

participating provider organizations that share patients and use a matching engine. A smartphone app vendor who may be able to adapt their existing products would also be needed.

Development and pilot testing should include a variety of implementation methods, such as use of QR codes or tapping phones using NFC communication. During this work, provider registration software vendors will need to write software to be able to communicate electronically with the patient's app. Specifically, the provider software will need to receive the correct identity information from the patient's app; store the information in the provider's registration software; confirm receipt of the information; return provider contact information to the app; and provide the app with instructions for how the patient can sign up for the provider's patient portal and link it to the app. Because current processes for patient portal sign-up vary, it may be important to conduct this development work in partnership with a diversity of providers and app vendors. As feasibility is demonstrated, pilot testing with new types of providers in different settings will help further refinement. It will also be important to assess if patients continue to use the app over time and identify the barriers to ongoing use.

Recommendation 3. Develop advanced app functionalities.

Stage 3 involves developing additional functionalities that could improve the uptake of the smartphone app and its potential for improving record matching. While we have focused on four advanced functionalities, others should also be developed to improve the value to patients and providers. Each of the four will require a development effort that would be undertaken by application designers, software developers, and other stakeholders (e.g., identity-proofing services, insurance companies, HINs), depending on the functionalities chosen and their requirements. The first two (establishing mechanisms to use the app for identity-proofing patients and creating a system in which login credentials could be used to log in to patient portals) are already under active discussion among stakeholders belonging to the CARIN Alliance and will be strengthened by emerging FIDO standards for simpler authentication. Once these functionalities are developed, they will require pilot testing to ensure usability without compromising security. Developing the third functionality (incorporating proof of insurance information into apps), will require involvement from insurance companies prior to pilot testing, and can be viewed as a logical extension of the Virtual Clipboard work already done by WEDI (though it has now stalled). While further automating the clipboard beyond identity information may be challenging, given the diversity across providers and the clipboard's function in workflows, doing so would generate substantial value to patients and should also be pursued. Finally, the development of the fourth functionality (using QHIN IDs for record matching) will likely require further input from stakeholders (such as providers, EHR vendors, app developers, HINs, and patient groups) for development of use cases and technical specifications prior to pilot testing, which can then be done within an interested HIN and participating providers.

Recommendation 4. Establish or designate an organization to oversee national progress in record matching.

Like many problems in health care, attempts to improve record matching have suffered from fragmentation, which impedes progress. When organizations, agencies, coalitions, developers, or providers launch initiatives and then abandon them without publishing "lessons learned" or retaining lessons in the form of institutional memory, any knowledge gained is wasted. Our findings suggest that record matching problems will not go away without the dedicated effort of a number of interested stakeholders for many years to come. Without a leading organization that convenes stakeholders, monitors and tracks progress, spreads best practices, and potentially helps establish governance processes (such as those for app certification), there is a risk that lessons will not be learned efficiently and record matching will never become a high priority for the public or for health system leaders. Such an organization could be public or private but should be recognized in some capacity by the federal government to provide legitimacy and promote transparency. This organization could be a new or existing entity and its role should evolve over time according to the needs of record matching efforts. Its work should not duplicate that of other organizations, such as standards development organizations. The organization could be established by making a long-term commitment to this issue and convening key stakeholders, or by being designated by the federal government.

Recommendation 5. Conduct more rigorous research into the nature and magnitude of record matching errors, and create methods for health care providers to objectively benchmark their record matching performance.

Record matching failure is a major safety and quality issue, yet very few studies have investigated its causes or measured organizational error rates; for their part, health care providers do not report them publicly. As a result, few patients seem to be aware of the problem. If there were a greater understanding of the extent of record matching failures, the public might demand solutions, and stakeholders (such as employers and other payers) would be more motivated to support (and pay for) them. Objective analysis of the financial and clinical burden associated with record matching failure may also motivate health care providers to address this problem. More rigorous research into the causes of record matching errors, development of methods for providers to benchmark their match error rates, and requirements to publicly report match rates would help provide much-needed transparency and would raise the profile of this issue. Data on match rates could also be used as part of a public awareness campaign to educate patients as to the severity of patient record matching problems and encourage them to participate in our proposed three-stage solution or other solutions.

Chapter Summary and Analysis

Our work has identified multiple potentially promising solutions to record matching in which the patient has some role beyond simply providing demographics. Although details of many of these solutions are limited, and assessments are inconclusive, it is likely that no patient-empowered solution is a "silver bullet," and improvements in record matching will require a constellation of solutions. We selected a three-stage approach that aims to improve the quality of identity information, establish new smartphone app functionality to facilitate bidirectional exchange of identity information and health care data between patients and providers, and create advanced functionality to further improve value. Advancing this solution will require development and pilot testing, and, likely, a governance mechanism. Other potential solutions we have identified, as well as those excluded from consideration due to scope, may also prove effective. For all the solutions that we identified, the lack of empirical assessments suggests that their potential to improve matching is largely unknown. Without more focused effort on developing and testing of the solutions we identified or others, current problems with record matching will likely remain the standard of care and continue to impede interoperability and HIE.

Appendix A. Glossary of Terms

American Society for Testing Materials (ASTM) standards—an internationally recognized set of voluntary consensus technical standards developed by ASTM for a wide range of materials, products, systems, and services.

Application Programming Interfaces (APIs)—a set of commands, functions, protocols, and objects that programmers can use to create software or interact with an external system.

Argonaut profiles—a set of profiles based on internet standards and architectural patterns and styles, which are used to rapidly develop a first-generation FHIR-based API and Core Data Services specification to enable expanded information sharing for EHRs and other health information technology.

Biometric data—a unique physical or behavioral characteristic (such as fingerprint) used especially as a means of verifying personal identity.

Check digits—a form of redundancy check used for error detection in identification numbers (such as bank account numbers).

Consolidated Clinical Document Architecture (CCDA)—an implementation guide that specifies a library of templates and prescribes their use for a set of specific document types.

Consumer-mediated exchange—an exchange of data that occurs when a patient manages his or her own data and sends it to chosen providers.

DIRECT message—a message sent using the DIRECT technical protocol, which allows writers to send secure patient information to other health care stakeholders.

Directed exchange—methods used by a health care provider to securely send patient information to another health care provider, care coordinator, or other stakeholder.

Fair Information Practice Principles—a set of principles developed by the FTC, which represent widely accepted concepts concerning fair information practice in an electronic marketplace. The major pillars include notice/awareness, choice/consent, access/participation, integrity/security, and enforcement/redress.

Fast Health Interoperability Resources (FHIR)—an interoperability standard for electronic exchange of health care information. FHIR was developed by Health Level Seven International (HL7), a not-for-profit organization that is accredited by the American National Standards

Institute and develops and provides frameworks and standards for the sharing, integration, and retrieval of clinical health data and other electronic health information.

Fast IDentity Online (FIDO) Alliance—an ecosystem for standards-based, interoperable authentication. The specifications and certifications from the FIDO Alliance enable an interoperable ecosystem of hardware-, mobile- and biometrics-based authenticators that can be used with many apps and websites.

Hash—the result of a mathematical algorithm that maps data of arbitrary size to a string of fixed size and is infeasible to invert.

Health information exchange (HIE)—the mobilization of health care information electronically across organizations within a region, community, or hospital system. In practice, the term "HIE" may also refer to the organization that facilitates the exchange.

Health information network (HIN)—broadly defined as the set of standards, specifications, and policies that enable the secure exchange of health information over the internet.

Health Level 7 (HL7)—a set of international standards for transfer of clinical and administrative data between software applications used by various health care providers.

Health record bank (HRB)—repository that stores a copy of the medical records that each of a patient's providers keeps for that patient. The patient controls who may access which parts of the information in his or her HRB account.

Identity assurance level (IAL)—refers to the identity-proofing process established by NIST. The IALs reflect the options government agencies may select from based on the agency's risk profile and the potential harm caused by an attacker making a successful false claim of an identity. They may be used by entities outside of government as well.

Knowledge-based identity information—identity information that is known by the patient, such as his or her mother's maiden name or city of birth.

Master patient index (MPI)—a database that maintains a unique index (or identifier) for every patient registered at a health care organization.

Matching engine—a set of algorithms used to match records together.

Metadata—a set of data that describes and gives information about other data.

National Institute of Standards and Technology (NIST)—a measurement standards laboratory and a nonregulatory agency of the United States Department of Commerce. Its mission is to promote innovation and industrial competitiveness.

Near-field communication (NFC)—a set of communication protocols that enable two electronic devices to establish communication by bringing them close together in space.

Patient-empowered approach—a method for matching records that gives the patient greater control and ownership of the matching process.

Personal health record (PHR)—an electronic, lifelong source of health information used by individuals to make health decisions. Individuals own and manage the information in the PHR, which may come from health care providers and from the individual. The PHR is maintained in a secure and private environment to which the individual determines rights of access. The PHR does not replace the legal record of any provider.

Public key—a cryptographic key that can be obtained and used by anyone to encrypt messages intended for a particular recipient, such that the encrypted messages can be deciphered only by using a second key that is known only to the recipient.

Public key cryptography—an encryption scheme that uses two mathematically related, but not identical, keys: a public key and a private key. Only the public key can decrypt a message that is encrypted with the private key and vice versa.

Qualified health information network (QHIN)—a HIN with additional required characteristics (as defined by TEFCA) for participating in data exchange among different networks.

Query-based exchange—an exchange of data that occurs when a provider requests information about a specific patient from another provider.

Quick response (QR) code—a machine-readable code consisting of an array of black and white squares, typically used for storing Uniform Resource Locators (URLs).

Recognized coordinating entity (RCE)—a governing body that is expected to operationalize the Trusted Exchange Framework by incorporating it into a single, all-encompassing Common Agreement to which QHINs agree to abide.

Record matching—the process of identifying records that refer to the same entity across different data sources (also known as "record linking").

Trusted Exchange Framework and Common Agreement (TEFCA)—a framework developed by the ONC to improve interoperability through the use of HINs. The framework will be governed by a recognized coordinating entity (RCE).

Voluntary universal identifier (VUID)—an identifier, such as a set of alphanumeric digits, that is unique to an individual.

Appendix B. Technical Expert Panel Members and Subject Matter Experts

Table B.1. Technical Expert Panel Members and Affiliations

Member Name	Affiliation
David W. Bates, M.D., M.Sc.	Brigham and Woman's Hospital
Doug Fridsma, M.D., Ph.D., F.A.C.P., F.A.C.M.I.	American Medical Informatics Association
Andrew Gettinger, M.D.	ONC
Leslie Kelly Hall	Healthwise
Cora Han, J.D.	FTC
Adam Landman, M.D., M.S., M.I.S., M.H.S.	Brigham and Woman's Hospital
David McCallie, M.D.	Cerner
Peter Szolovits, Ph.D.	Massachusetts Institute of Technology

Table B.2. Subject Matter Experts and Affiliations

Name	Affiliation
Dixie Baker, Ph.D.	Martin, Blanck and Associates
Robert Cothren, Ph.D.	National Association for Trusted Exchange
Adrian Gropper, M.D.	Patient Privacy Rights
Barry Hieb, M.D.	GPII
Ryan Howells, M.H.A.	Leavitt Partners
Beth Just, M.B.A, R.H.I.A., F.A.H.I.M.A.	Just Associates
Robert Klootwyk	Epic Health Systems
Matt Doyle	Epic Health Systems
Janet Campbell	Epic Health Systems
Lyndee Knox	LA Net
Adam Landman, M.D., M.S., M.I.S., M.H.S.	Brigham and Woman's Hospital
Bradley Malin, Ph.D.	Vanderbilt University
Carolyn Peterson, M.S., M.B.I.	Mayo Clinic Global Business Solutions
William Yasnoff, M.D., Ph.D.	National Health Information Infrastructure (NHII) Advisors
Eric Heflin	The Sequoia Project
Jitin Asnaani, M.B.A.	CommonWell Health Alliance
Catherine Schulten	LifeMed ID, Inc.
Devin Jopp, Ed.D.	The American College Health Association (ACHA)

Table B.2—Continued

Name	Affiliation
David McCallie, M.D.	Cerner
Tim Pletcher, M.D.	Michigan Health Information Network Shared Services (MiHIN)
Courtney Delgoffe	MiHIN
Aaron Miri, M.B.A.	Imprivata, Inc.
Arien Malec	RelayHealth
Deb Bass	Nebraska Health Information Initiative (NeHII)
Josh Mandel, M.D.	Google, Harvard Medical School
Michael Hodgkins, M.D.	Xcertia
Cora Han, J.D.	FTC
Andrew Gettinger, M.D.	ONC
Jared Esposito, P.M.P.	Athenahealth, Inc.
Keith Hanna, Ph.D.	Intellectual Property, Research, Deployment (IPRD) Group
Sarvesh Makthal	IPRD Group

NOTE: One SME requested anonymity.

Appendix C. Literature Search Terms

PubMed
2007–present; English
July 21, 2017

"patient matching" OR (patient[title/abstract] AND "record matching") OR (health[title/abstract] AND "record matching") OR "universal patient identifier" OR (patient-managed[title/abstract] AND identifier[title/abstract]) OR (patient-managed[title/abstract] AND "identification system"[title/abstract]) OR (voluntary[title/abstract] AND "patient identifier"[title/abstract]) OR (voluntary[title/abstract] AND "universal identifier"[title/abstract]) OR (voluntary[title/abstract] AND universal[title/abstract] AND health care[title/abstract] AND identifier[title/abstract]) OR (voluntary[title/abstract] AND universal[title/abstract] AND health care[title/abstract] AND identification[title/abstract]) OR (universal[title/abstract] AND health care[title/abstract] AND identifier[title/abstract]) OR (universal[title/abstract] AND "health-care identifier"[title/abstract]) OR (universal[title/abstract] AND "health care identifier"[title/abstract]) OR (universal[title/abstract] AND "personal identifier"[title/abstract]) OR "health record bank" OR "personally controlled health record" OR "personally controlled health records"

ACM Digital Library
2007–present
July 21, 2017

"patient matching" OR "patient record matching" OR "health record matching" OR "universal patient identifier" OR "patient-managed identifier" OR "patient-managed identification system" OR "voluntary patient identifier" OR "voluntary universal identifier" OR "voluntary universal health care identifier" OR "voluntary universal health care identification" OR "universal health care identifier" OR "universal health-care identifier" OR "universal health care identifier" OR "universal personal identifier" OR "health record bank" OR "personally controlled health record" OR "personally controlled health records"

IEEE
2007–present
July 21, 2017

"patient matching" OR "patient record matching" OR "health record matching" OR "universal patient identifier" OR "patient-managed identifier" OR "patient-managed identification system" OR "voluntary patient identifier" OR "voluntary universal identifier"

OR “voluntary universal health care identifier” OR “voluntary universal health care identification” OR “universal health care identifier” OR “universal health-care identifier” OR “universal health care identifier” OR “universal personal identifier” OR “health record bank” OR “personally controlled health record” OR “personally controlled health records”

Web of Science
2007–present; English
July 21, 2017

TOPIC: (“patient matching”) OR TOPIC: (“patient record matching”) OR TOPIC: (“health record matching”) OR TOPIC: (“universal patient identifier”) OR TOPIC: (“patient-managed identifier”) OR TOPIC: (“patient-managed identification system”) OR TOPIC: (“voluntary patient identifier”) OR TOPIC: (“voluntary universal identifier”) OR TOPIC: (“voluntary universal health care identifier”) OR TOPIC: (“voluntary universal health care identification”) OR TOPIC: (“universal health care identifier”) OR TOPIC: (“universal health-care identifier”) OR TOPIC: (“universal health care identifier”) OR TOPIC: (“universal personal identifier”) OR TOPIC: (“health record bank”) OR TOPIC: (“personally controlled health record”) OR TOPIC: (“personally controlled health records”)

Appendix D. Literature Search Results

Table D.1. U.S.-Based Literature

Author	Title	Publication Year	Summary
Alreja et al.	"Reducing Patient Identification Errors Related to Glucose Point-of-Care Testing"	2011	Evaluation of a commercial automated bar code solution that adds extra check for identity.
Appavu	"Analysis of Unique Patient Identifier Options"	1997	Analyzes aspects of UPIs and offers detailed analyses of 13 specific options proposed by various organizations and individuals. Includes identification for care and for administrative purposes.
Bishop and Holms	"National Consumer Heath Privacy Survey"	2005	Survey of national consumers and California residents on health information privacy.
Bourgeois, Taylor, et al.	"Whose Personal Control? Creating Private, Personally Controlled Health Records for Pediatric and Adolescent Patients	2008	Analysis of access control policies and content for creating a personally controlled health record (PCHR) for adolescents.
Bourgeois, Mandl et al.	"Mychildren's: Integration of a Personally Controlled Health Record with a Tethered Patient Portal for a Pediatric and Adolescent Population"	2009	Description of design for integrating a PCHR for children into one institution's her.
Caine and Hanania	"Patients Want Granular Privacy Control over Health Information in Electronic Medical Records"	2013	Survey of patients' preferences for the level of control over health information on an electronic medical record.
Caine et al.	"Designing a Patient-Centered User Interface for Access Decisions About EHR Data: Implications from Patient Interviews"	2015	User needs assessment and concept user interface mockups to allow patient control of access to medical records.
Chen and Zhong	"Emergency Access Authorization for Personally Controlled Online Health Care Data"	2012	Proposes novel method for determining if provider should have access to patient health record in emergency situations.
Cimino et al.	"Consumer-Mediated Health Information Exchanges"	2014	Debate summary of the shift to a consumer-mediated exchange in HIE organizations.
Culbertson et al.	"The Building Blocks of Interoperability: A Multisite Analysis of Patient Demographic Attributes Available for Matching"	2017	Study to determine what patient demographic attributes are collected at multiple institutions and how those attributes varied across clinical sites.

Table D.1—Continued

Author	Title	Publication Year	Summary
Davidson and Durkin	"Evaluation of the WHIN/GPII VUHID Demonstration Project"	2013	Evaluation of GPII's system of a VUID universal identifier in three health systems as part of an HIE in California.
Dooling et al.	"Survey: Patient Matching Problems Routine in Health Care"	2016	Survey showing half of one organization's members work on duplicate records, with three-quarters doing so weekly.
Goldstein et al.	*Data Segmentation in Electronic Health Information Exchange: Policy Considerations and Analysis*	2010	Summarizes issues with data segmentation and challenges to consider for policies on segmentation, including issues around access and data exchange.
Hembroff	"Improving Patient Safety, Health Data Accuracy, and Remote Self-Management of Health Through the Establishment of a Biometric-Based Global UHID"	2016	Technical description of an 82-digit ID generated from a person's eight fingerprints.
HHS	*Unique Health Identifier for Individuals*	1998	Proposed rule describing the need for a unique health identifier (UHID) with parameters and criteria for any UHID, including several suggestions.
Hieb	"A Cost Effective Method to Create a Universal Health Care Identifier System"	2010	Discusses the model for GPII's voluntary identifier and cost analysis.
Hieb and West	"The Role of Unique Individual Identifiers in Facilitating Healthcare Interoperability"	2012	Discusses the need for a universal identifier that is supported by enterprise master patient index in terms of cost savings and better patient care.
Hillestad, Bigelow, Chaudry, et al.	*Identity Crisis: An Examination of the Costs and Benefits of a Unique Patient Identifier for the U.S. Health Care System*	2008	Compares a UPI with statistical methods for patient matching in terms of error rate, cost, privacy, information security, and political consideration as well as the operational efficiency, ease of implementation, and implications for improved health care for a UPI.
Just et al.	"Why Patient Matching Is a Challenge: Research on Master Patient Index (MPI) Data Discrepancies in Key Identifying Fields"	2016	Study to examine the underlying causes of duplicate records using a multisite data set of 398,939 patient records with confirmed duplicates and analyzed multiple reasons for data discrepancies between those record matches.
Lapsia, Lamb, and Yasnoff	"Where Should Electronic Records for Patients Be Stored?"	2012	Simulation of centralized versus distributed storage of EHRs.
Leonard, Pons, and Asfour	"Realization of a Universal Patient Identifier for Electronic Medical Records Through Biometric Technology"	2009	Proposes a theoretical matching framework using biometrics (fingerprints at first) followed by demographic and blood-type matching.

Table D.1—Continued

Author	Title	Publication Year	Summary
Leventhal et al.	"Designing a System for Patients Controlling Providers' Access to Their Electronic Health Records: Organizational and Technical Challenges"	2015	Design decisions and rationale for giving patient's granular control of HIE data available to clinicians in one clinic.
Mandl et al.	"Indivo: A Personally Controlled Health Record for Health Information Exchange and Communication"	2007	Overview of the design of a PCHR.
Meslin et al.	"Giving Patients Granular Control of Personal Health Information: Using an Ethics 'Points to Consider' to Inform Informatics System Designers"	2013	Develops a tool for ethical considerations of any effort to develop a method to provide patient with more granular EHR control.
Muntz	"Thoughts and Recommendations on a National Health Safety Identifier"	2016	Highlights issues with misidentification and advocates a patient-led and -managed health safety identifier using biometrics.
Ponemon Institute	*2016 National Patient Misidentification Report*	2016	Identifies causes and outcomes of misidentification and how some issues can be remedied.
Schwartz et al.	"Patient Preferences in Controlling Access to Their Electronic Health Records: A Prospective Cohort Study in Primary Care"	2015	Assessment of patients' choices for and perspectives on controlling access to their records at one clinic.
Tierney et al.	"Provider Responses to Patients Controlling Access to Their Electronic Health Records: A Prospective Cohort Study in Primary Care"	2015	Evaluation of one clinic that implemented giving patients access control to parts of their records to providers in the clinic.
Weitzman, Kaci, and Mandl	"Acceptability of a Personally Controlled Health Record in a Community-Based Setting: Implications for Policy and Design"	2009	Qualitative study of perspectives on PCHR.
Weitzman, Kaci, et al.	"Helping High-Risk Youth Move Through High-Risk Periods: Personally Controlled Health Records for Improving Social and Health Care Transitions"	2011	Overview of PCHR and how it satisfies the chronic care model.
Weitzman, Kelemen, et al.	"Willingness to Share Personal Health Record Data for Care Improvement and Public Health: A Survey of Experienced Personal Health Record Users"	2012	Survey of users of a PCHR regarding perceptions of sharing.

Table D.1—Continued

Author	Title	Publication Year	Summary
WEDI	"Virtual Clipboard Initiative Launched to Streamline Patient Intake and Eliminate Wasteful Administrative Processes"	2015	Describes the pilot functionality for a Virtual Clipboard based on stakeholder involvement, with the initial goal of sharing information contained on an insurance card between patients, providers, and payers, and gradually increasing functionality.
Yasnoff and Shortliffe	"Lessons Learned from a Health Record Bank Start-Up"	2014	Description of an HRB model startup that was attempted and failed due to lack of revenue.
Zech et al.	"Identifying Homelessness Using Health Information Exchange Data"	2015	Analysis of homeless registrations in an HIE.
Zhang et al.	"Emergency Access for Online Personally Controlled Health Records System"	2012	Describes a method for granting access to providers in a "break-the-glass" situation by polling trusted individuals.

Table D.2. Non-U.S.-Based Literature

Author	Title	Publication Year	Country	Summary
Abdulnabi et al.	"A Distributed Framework for Health Information Exchange Using Smartphone Technologies"	2017	Malaysia	Describes technology for how patient smartphones can be used to implement HRBs.
Alnuem et al.	"Towards Integrating National Electronic Care Records in Saudi Arabia"	2012	Saudi Arabia	Discusses the criteria needed for a unique patient identifier and how that can be adapted for the Saudi Arabian health system.
Dixon	"A Failure to 'Do No Harm'—India's Aadhaar Biometric ID Program and Its Inability to Protect Privacy in Relation to Measures in Europe and the U.S."	2017	India	Review of the Republic of India's national digital biometric identity system, the Aadhaar, for its development, data protection and privacy policies, and impact.
Fernandes and O'Connor	"Accurate Patient Identification—A Global Challenge"	2015	Global	Summarizes patient identification strategies used in multiple countries (Singapore, Canada, Australia, and Wales).
Grunwell et al.	"Managing and Sharing Health Data Through Information Accountability Protocols"	2015	Australia	Reviews the Information Accountability Framework and how it was implemented in a customized EHR to balance patient control of health information and access to information needed for clinical care by providers.

Table D.2—Continued

Author	Title	Publication Year	Country	Summary
Health Information Quality Authority	"Recommendations for a Unique Health Identifier for Individuals in Ireland"	2009	Ireland	Reviews the current recommendations for a UHID in Ireland and highlights its shortfalls based on criteria laid out in the report.
Plischke et al.	"The Lower Saxony Bank of Health: Rationale, Principles, Services, Organization and Architectural Framework"	2014	Germany	Description of a plan for an HRB in Germany.
Rostad and Nytro	"Personalized Access Control for a Personally Controlled Health Record"	2008	Norway	Proposed access control framework and rules for a PCHR.

Appendix E. Evaluation of Each Solution by Criteria

This appendix consists of two tables. Table E.1 shows the results of applying all of the 11 evaluation criteria to each of the first six solutions. Table E.2 presents similar results for the remaining four solutions. The contents of the table was derived from the author's analysis of the literature and expert input, and contains only brief summaries of findings.

Table E.1. Solutions 1 Through 6 Evaluated by Criteria

Criteria	Solution 1: Voluntary Universal Identifier	Solution 2: Public Key	Solution 3: Government-Issued ID	Solution 4: Knowledge-Based Identity Information	Solution 5: Biometric data	Solution 6: Verify Identity
Criterion 1: Improvement in record matching	Unique identifier would result in perfect matching for every health care encounter in which it is used properly	Unique key would result in perfect matching for every health care encounter in which it is used properly, but only for patients with access to the technology (smartphone)	Identifiers would improve matching, but patients may use different identifiers at different times	Knowledge-based data may improve record matching somewhat	High and increasing potential to improve match rates, but no biometrics are perfect and some do not work as well for some patient types (e.g., minorities for facial recognition)	High potential to improve match rates and indicates data quality of identifying information; improvement will vary based on information type (e.g., mobile phone numbers change); requires technology (e.g., mobile phone)
Criterion 2: Patient control	Private identifiers, if supported by providers and used properly by patients, afford granular patient control at the time of an encounter	Potential for patients to segment record using multiple keys	Minimal patient control except for the ability to opt out; even then, patients may not realize they can opt out	Minimal patient control except for the ability to opt out	Minimal patient control except for the ability to opt out	Minimal patient control except for the ability to opt out
Criterion 3: Likelihood of adoption by patients	Easy for patients to understand how to use it, but some may not want another identifier; potential for simplified clipboard process	Unlikely except with highly motivated patients because value proposition is not well defined	Likely because government already typically provides such identifiers (however some patients lack government-issued IDs)	Likely because of low burden and is easy to understand	Likely because of convenience and increasing comfort with supplying biometrics in other settings, but may be less likely if patients were better aware of the different ways biometric data was shared	If verification process is minimally burdensome (e.g., responding to a text message), adoption will likely be high

Table E.1—Continued

Criteria	Solution 1: Voluntary Universal Identifier	Solution 2: Public Key	Solution 3: Government-Issued ID	Solution 4: Knowledge-Based Identity Information	Solution 5: Biometric data	Solution 6: Verify Identity
Criterion 4: Likelihood of adoption by providers	Would require major change in front desk workflow and so would need strong leadership support; uncertain willingness to support data segmentation; some concern about dependency on a central organization	Unlikely because value proposition is not well defined	Unlikely because of extra workflow step to enter identifiers	Unlikely without strong leadership support because of additional workflow step.	Cost of equipment and changes in workflows may be strong barriers for some providers, especially in under-resourced settings	May require some change in workflows depending on method of verification, but otherwise reasonable chance of adoption
Criterion 5: Likelihood of adoption by vendors	EHR vendors would likely need to add new identifier field, which should be relatively easy technically; hardware and software supplied by central system	EHR vendors would need to implement new software functionality to support keys and workflows	Would be relatively easy to add new field	Would be relatively easy to add new field	Adding standardized biometric data would require some software development, but would be relatively easy if specifications were well defined (depending on technical architecture)	Would require implementation of new metadata fields, which would be technically easy if specifications were established
Criterion 6: Feasibility	Only requires willing providers for more pilot testing	Management of keys may be complicated and need to be centrally managed	Relatively simple because many government-issued IDs already exist	Pilot testing would be feasible once data elements were established	Will likely be challenging to come to agreement among multiple vendors on which data type, format, and privacy policies to use, new or emerging technical architectures may address some barriers	Developing verification processes will require some development but are already common in other industries and likely to be minimally burdensome
Criterion 7: Minimal security risks	Central organization raises concern, but lack of personally identifiable information (PII) stored centrally and easy ability to replace identifiers mitigates concerns	Private keys would need to be kept secure, but cryptography would prevent fraudulent uses of IDs	Storing a new form of PII may increase risk somewhat	Increased use of data elements that are currently used for authentication and identity-proofing is probably poor security practice	Risk of data breach increases with data that is nonrepudiatable, and sharing more widely may increase opportunity for fraud	The additional verification process and metadata would not likely increase security risks but may depend on implementation details

Table E.1—Continued

Criteria	Solution 1: Voluntary Universal Identifier	Solution 2: Public Key	Solution 3: Government-Issued ID	Solution 4: Knowledge-Based Identity Information	Solution 5: Biometric data	Solution 6: Verify Identity
Criterion 8: Sustainability	Unclear business model to pay for identity-proofing, hardware, software, and operational costs; uncertain if front desk staff will effectively manage identifiers in distributed fashion	Unclear costs required if central organization is responsible for managing keys	Minimal ongoing costs or barriers to sustainability once software and processes are in place	Minimal ongoing costs or barriers to sustainability once software and processes are in place	Minimal ongoing costs or barriers to sustainability once software, hardware, and processes are in place	Minimal ongoing costs or barriers to sustainability once software and processes are in place
Criterion 9: Political viability	Already completed consensus process on identifier format, and can be piloted and spread starting from small number of providers; unclear governance process needed to maintain	Would likely need consensus on technical specifications for keys and workflows for using them, which may be challenging	Minimal challenges because IDs are already collected	Requires consensus on small number of knowledge-based data elements, which may be difficult to achieve	Defining open specifications and governance process with diverse vendors may be very challenging, and privacy concerns may result in pushback until strong privacy protections exist	Requires open technical specifications and agreement about meaning of metadata fields
Criterion 10: Potential to foster new uses of data	Does not directly foster new uses of matched data other than through facilitating assembly of complete records that could be used for other purposes	Does not directly foster new uses of matched data other than through facilitating assembly of complete records that could be used for other purposes	Does not directly foster new uses of matched data other than through facilitating assembly of complete records that could be used for other purposes	Does not directly foster new uses of matched data other than through facilitating assembly of complete records that could be used for other purposes	Does not directly foster new uses of matched data other than through facilitating assembly of complete records that could be used for other purposes	Does not directly foster new uses of matched data other than through facilitating assembly of complete records that could be used for other purposes
Criterion 11: Low potential for negative unintended consequences	Unknown but may include over-reliance on one identifier, fraudulent use, and confusion about segmentation	Unknown because solution is relatively unspecified	Unknown but likely minimal	Unknown but likely minimal	Unknown but potential issues with certain minorities (for facial data matching) and a privacy backlash if patients are not properly informed	Unknown but likely minimal

Table E.2. Solutions 7 Through 10 Evaluated by Criteria

Criteria	Solution 7: Consumer-Directed Exchange	Solution 8: HRBs	Solution 9: Patients Manually Verify Matches	Solution 10: Patients Supply Record Location
Criterion 1: Improvement in record matching	Would reduce need for matching engines because patients would supply record contents directly	Would reduce need for matching engines because patients would supply record contents or identifier from HRB	May help with false positives but not as much with false negatives because of privacy restrictions	May help improve matching somewhat when patients correctly recall locations of their previous visits
Criterion 2: Patient control	Potential for complete patient control over records	Potential for complete patient control over records	May allow patients to hide a record that they want to keep private	Patient may be allowed to designate certain locations as private or not reveal them
Criterion 3: Likelihood of adoption by patients	Previous attempts at PHRs suggest few patients may be motivated to use but facilitating access to data may improve adoption	Previous attempts at HRBs suggests few patients may be motivated to use but if data were collected regionally more may be interested	Likely only small numbers of motivated patients would do the extra work to verify matches	Patients may be confused about why they need to supply this information
Criterion 4: Likelihood of adoption by providers	Would require providers to integrate patient-collected data into workflows, which is a large barrier; ability to restrict access to data may reduce provider willingness to adopt	Providers may not trust a third party to curate and manage their data for them	Would require new work processes and support for incorporating patient's input, which may be cumbersome	Would require new work processes and support for incorporating patient's input, which may be cumbersome
Criterion 5: Likelihood of adoption by vendors	App vendors will be eager to have access to data; EHRs and HIEs may be reluctant to support new workflows without clear value proposition	A vendor would be needed to support infrastructure for a region, and EHR vendors may be reluctant to integrate with it for competitive reasons	Would require some software development to allow patient to provide input	Would require some software development to allow patient to provide location information
Criterion 6: Feasibility	Assembling data and integrating it back into providers' workflows will require new technical specifications and processes	Requires new technical infrastructure and processes, which will likely involve considerable costs	Pilot testing would be feasible once software was developed	Pilot testing would be feasible once software and work processes were developed

Table E.2—Continued

Criteria	Solution 7: Consumer-Directed Exchange	Solution 8: HRBs	Solution 9: Patients Manually Verify Matches	Solution 10: Patients Supply Record Location
Criterion 7: Minimal security risks	Introduces target of data not protected by HIPAA	Introduces target of data (which may be protected by HIPAA)	Minimal risks	Minimal risks
Criterion 8: Sustainability	Unclear business model and unknown ongoing costs	Unclear business model and unknown ongoing costs	Minimal ongoing costs or barriers to sustainability once software and processes are in place	Minimal ongoing costs or barriers to sustainability once software and processes are in place
Criterion 9: Political viability	Strong support for giving patients access to and control of their data among some groups, but uncertain support from providers or other stakeholders	Questionable support for a regional aggregation of data and consensus among providers to participate	Minimal challenges	Minimal challenges
Criterion 10: Potential to foster new uses of data	High potential for new uses because of existence of complete longitudinal health record	High potential for new uses because of existence of complete longitudinal health record	Does not directly foster new uses of matched data other than through facilitating assembly of complete records that could be used for other purposes	Does not directly foster new uses of matched data other than through facilitating assembly of complete records that could be used for other purposes
Criterion 11: Low potential for negative unintended consequences	Unknown but may involve unexpected uses of aggregated data	Unknown but may involve unexpected uses of aggregated data	Unknown but likely minimal	Unknown but likely minimal

Appendix F. Blockchain-Based Solution

Several experts mentioned the potential to use emerging blockchain technology as a part of a record matching solution, and many white papers (but only a few very recent peer-reviewed research studies) have been published describing proof of concepts or early implementations (Ryan, 2017; Deshpande et al., 2017; "Blockchain in Healthcare Today," 2018). Because blockchain is still a relatively new technology with many challenges, and at the advice of our expert panel, we did not focus on this solution in our report. Nevertheless, we recognize its potential to serve a role in the future and so briefly describe how blockchain-based solutions may be relevant to patient record matching as well as the challenges that such solutions may face.

A blockchain is a distributed, shared database that allows participants to perform transactions without requiring a central organization to vouch for the transactions' validity. The data is replicated across the network so that every node has a complete copy of all transactions. The result is that transactions are validated and cannot be repudiated. A blockchain alone cannot improve record matching, just as any database alone cannot improve matching. However, a blockchain has the potential to be used as part of a solution to remove the dependence on a central organization for certain functions.

Several proposals describe how blockchain-based solutions could help implement a PHR functionality by facilitating nonrepudiatable information exchange and transactions (e.g., prescriptions) among patients, providers, and other health care stakeholders, allowing patients to control their data without the need for any intermediary institutions ("HIE of One," 2017; Gropper and the Loop Project Team, 2017). To improve record matching, such an approach would still encounter some of the challenges of any PHR solution that we identified in the main text: aggregating the data in the patient's account, and integrating the patient-controlled data into providers' workflows. Although blockchain-based solutions may remove the need for a central organization to manage consent and access control, the guidelines and protocols for those processes must be established and widely agreed upon. Otherwise, providers may refuse to accept the data (Tierney et al., 2015). Developing the access control guideline and protocols will be a complex task, which cannot be addressed solely with technology innovations, and may require a governing organization to make ongoing decisions. The need for a central governing organization somewhat reduces the main benefit of a blockchain approach (Gordon, Wright, and Landman, 2017).

Blockchain also introduces new challenges. For example, account recovery in the event that a patient lost his or her blockchain password or keys must be feasible. One option that is being explored is a social identity recovery mechanism in which a patient's family members vote to verify the patient's identity. Two articles in the literature describe similar mechanisms in which family members could vote to verify an identity in emergency situations (Chen and Zhong, 2012;

Zhang et al., 2012). Other challenges include cost to maintain infrastructure, given that some blockchain implementations require substantial electronic storage and computational resources, as well as computational performance limitations.

As with other solutions we identified, blockchain-based solutions are also likely not "silver bullets" for patient record matching. While blockchain has the potential to address some trust issues by reducing reliance on a central organization, further questions remain as to whether the technology, governance, and workflow barriers can be overcome.

References

21st Century Cures Act of 2016—*See* Public Law 114-255.

Abdulnabi, Mohamed, Ahmed Al-Haiqi, M. L. M. Kiah, A. A. Zaidan, B. B. Zaidan, and Muzammil Hussain, "A Distributed Framework For Health Information Exchange Using Smartphone Technologies," *Journal of Biomedical Informatics*, Vol. 69, No. C, 2017, pp. 230–250.

AHIMA e-HIM Personal Health Record Work Group, "Defining the Personal Health Record," *Journal of the American Medical Informatics Association*, Vol. 76, No. 6, 2005, pp. 24–25.

Alnuem, Mohammed, Samir El-Masri, Ahmed Youssef, and Ahmed Emam, "Towards Integrating National Electronic Care Records in Saudi Arabia," *International Conference on Bioinformatics and Computational Biology*, 2012, pp. 777–782.

Alreja, G., N. Setia, J. Nichols, and L. Pantanowitz, "Reducing Patient Identification Errors Related to Glucose Point-of-Care Testing," *Journal of Pathology Informatics*, Vol. 2, 2011, p. 22.

Anderson, Monica, "Digital Divide Persists Even as Lower-Income Americans Make Gains in Tech Adoption," 2017. http://www.pewresearch.org/fact-tank/2017/03/22/digital-divide-persists-even-as-lower-income-americans-make-gains-in-tech-adoption/

Anderson, Monica, and Andrew Perrin, "Tech Adoption Climbs Among Older Adults," Pew Research Center, 2017. http://www.pewinternet.org/2017/05/17/tech-adoption-climbs-among-older-adults/

Appavu, Soloman I., *Analysis of Unique Patient Identifier Options*, Washington, D.C.: U.S. Department of Health and Human Services, 1997.

Bell, Sigall K., Tom Delbanco, and Jan Walker, "OpenNotes: How the Power of Knowing Can Change Health Care," *NEJM Catalyst*, 2017. https://catalyst.nejm.org/opennotes-knowing-change-health-care/

Bipartisan Policy Center, *Challenges and Strategies for Accurately Matching Patients to Their Health Data*, Washington, D.C.: Bipartisan Policy Center, 2012.

Bishop, L., and B. Holms, *National Consumer Heath Privacy Survey*, Oakland, CA: California HealthCare Foundation, 2005.

"Blockchain in Healthcare Today," 2018. As of May 8, 2018: https://blockchainhealthcaretoday.com/index.php/journal

"Blue Button," 2017. As of May 8, 2018:
https://www.healthit.gov/topic/health-it-initiatives/blue-button

Blumenthal, David, "In Conversation with . . . David Blumenthal, M.D., MPP," in Robert W. Wachter, ed., *Perspectives on Safety*, Washington, D.C.: Agency for Healthcare Research and Quality, 2018.
https://psnet.ahrq.gov/perspectives/perspective/248

Boden, Rian, "Apple Pay In-Store Adoption Is 'Growing Nicely,'" 2017.
https://www.nfcworld.com/2017/03/30/351377/apple-pay-in-store-adoption-is-growing-nicely/

Bourgeois, F. C., K. D. Mandl, D. Shaw, D. Flemming, and D. J. Nigrin, "MyChildren's: Integration of a Personally Controlled Health Record with a Tethered Patient Portal for a Pediatric and Adolescent Population," *AMIA Annual Symposium Proceedings*, Vol. 2009, November 14, 2009, pp. 65–69.
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2815447/pdf/amia-f2009-65.pdf

Bourgeois, F. C., P. L. Taylor, S. J. Emans, D. J. Nigrin, and K. D. Mandl, "Whose Personal Control? Creating Private, Personally Controlled Health Records for Pediatric and Adolescent Patients," *Journal of the American Medical Informatics Association*, Vol. 15, No. 6, 2008, pp. 737–743. As of July 25, 2018:
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2585529/pdf/737.S1067502708001412.main.pdf

Caine, K., and R. Hanania, "Patients Want Granular Privacy Control over Health Information in Electronic Medical Records," *Journal of the American Medical Informatics Association*, Vol. 20, No. 1, January 1, 2013, pp. 7–15.

Caine, Kelly, Spencer Kohn, Carrie Lawrence, Rima Hanania, Eric M. Meslin, and William M. Tierney, "Designing a Patient-Centered User Interface for Access Decisions About EHR Data: Implications from Patient Interviews," *Journal of General Internal Medicine*, Vol. 30, No. 1, January 1, 2015, pp. 7–16.

CARIN Alliance, "CARIN Alliance," 2017. As of October 10, 2017:
http://carinalliance.com/

———, "Trusted Framework Principles for Consumer Directed Exchange," 2018. As of May 21, 2018:
http://carinalliance.com/trust-framework-principles/

CFR—*See* Code of Federal Regulations.

Chen, T., and S. Zhong, "Emergency Access Authorization for Personally Controlled Online Health Care Data," *Journal of Medical Systems*, Vol. 36, No. 1, February 2012, pp. 291–300. https://link.springer.com/content/pdf/10.1007%2Fs10916-010-9475-2.pdf

Chew, Hanley, and Eric Ball, "The Impact of the Surge of Biometric Data Privacy Lawsuits Against Employers," 2018. As of May 2, 2018: http://www.lawjournalnewsletters.com/sites/lawjournalnewsletters/2018/01/01/the-impact-of-the-surge-of-biometric-data-privacy-lawsuits-against-employers/?slreturn=20180402165849

CHIME—*See* College of Health Care Information Management Executives.

Cimino, James J., Mark E. Frisse, John Halamka, Latanya Sweeney, and William Yasnoff, "Consumer-Mediated Health Information Exchanges," *Journal of Biomedical Informatics*, Vol. 48, No. C, 2014, pp. 5–15.

Code of Federal Regulations, Health Breach Notification Rule; Final Rule, Vol. 74, No. 163, 2009.

College of Health Care Information Management Executives, *Summary of CHIME Survey on Patient Data-Matching*, Arlington, VA: College of Healthcare Information Management Executives, 2012. https://chimecentral.org/wp-content/uploads/2014/11/Summary_of_CHIME_Survey_on_Patient_Data.pdf

"Cross-Community Patient Discovery," 2017. As of May 2, 2018: https://wiki.ihe.net/index.php/Cross-Community_Patient_Discovery

Culbertson, A., S. Goel, M. B. Madden, N. Safaeinili, K. L. Jackson, T. Carton, R. Waitman, M. Liu, A. Krishnamurthy, L. Hall, N. Cappella, S. Visweswaran, M. J. Becich, R. Applegate, E. Bernstam, R. Rothman, M. Matheny, G. Lipori, J. Bian, W. Hogan, D. Bell, A. Martin, S. Grannis, J. Klann, R. Sutphen, A. B. O'Hara, and A. Kho, "The Building Blocks of Interoperability: A Multisite Analysis of Patient Demographic Attributes Available for Matching," *Applied Clinical Information*, Vol. 8, No. 2, 2017, pp. 322–336.

Davidson, S. M., and S. Durkin, *Evaluation of the WHIN/GPII VUHID Demonstration Project*, Kansas City, MO: Durkin & Associates, 2013.

Deshpande, Advait, Katherine Stewart, Louise Lepetit, and Salil Gunashekar, *Distributed Ledger Technologies/Blockchain: Challenges, Opportunities, and the Prospect for Standards*, London: British Standards Institute, 2017.

Dixon, Pam, "A Failure to 'Do No Harm'—India's Aadhaar Biometric ID Program and Its Inability to Protect Privacy in Relation to Measures in Europe and the U.S," *Health and Technology*, Vol. 7, No. 4, February 2012, pp. 539–567.

Dooling, Julia, Lorraine Fernanded, Annessa, Grant Landsbach, Katherine Lusk, Megan Munns, Meysa Noreen, Michele O'Conner, and Melinda Patten, "Survey: Patient Matching Problems Routine in Healthcare," 2016. http://journal.ahima.org/2016/01/06/survey-patient-matching-problems-routine-in-healthcare/

Federal Trade Commission, *Complying with the FTC's Health Breach Notification Rule*, 2010. https://www.ftc.gov/tips-advice/business-center/guidance/complying-ftcs-health-breach-notification-rule

Fernandes, Lorraine, and Michele O'Connor, "Accurate Patient Identification—A Global Challenge," *AHIMA Perspectives in Health Information Management*, 2015, pp. 1–7.

"FHIR Release 3 (STU)," 2017. As of May 2, 2018: https://www.hl7.org/fhir/overview.html

"FIDO Alliance," 2018. As of May 21, 2018: https://fidoalliance.org/

FTC—*See* Federal Trade Commission.

Goldstein, M. M., A. L. Rein, M. M. Heesters, P. P. Hughes, B. Williams, and S. A. Weinstein, *Data Segmentation in Electronic Health Information Exchange: Policy Considerations and Analysis*, Washington, D.C.: U.S. Department of Health and Human Services, Office of the National Coordinator for Health IT, 2010.

Gordon, William, Adam Wright, and Adam Landman, "Blockchain in Health Care: Decoding the Hype," *NEJM Catalyst*, 2017. https://catalyst.nejm.org/decoding-blockchain-technology-health/

"GPII, Inc.," 2013. As of May 1, 2018: https://gpii.info/

Greenberg, Michael D., and M. Susan Ridgely, "Patient Identifiers and the National Health Information Network: Debunking a False Front in the Privacy Wars," *Journal of Health & Biomedical Law*, Vol. 4, No. 1, 2008, pp. 31–68.

Greenberg, M. D., M. Susan Ridgely, and Richard J. Hillestad, "Crossed Wires: How Yesterday's Privacy Rules Might Undercut Tomorrow's Nationwide Health Information Network," *Health Affairs*, Vol. 28, No. 2, 2009, pp. 450–452.

Gropper, Adrian, and the Loop Project Team, *HIE of One Loop: A Patient-Controlled Independent Health Record*, 2017. https://drive.google.com/file/d/0B_Rve6d1gHMWNmtueU5mTm9wVEk/view

Grunwell, D., P. Batista, S. Campos, and T. Sahama, "Managing and Sharing Health Data Through Information Accountability Protocols," *2015 17th International Conference on E-health Networking, Application & Services (HealthCom)*, 2015, pp. 200–204.

Health Information and Quality Authority, *Recommendations for a Unique Health Identifier for Individuals in Ireland*, Mahon, Cork, Ireland: Health Information and Quality Authority, 2009.

"Health Record Banks FAQs," 2016. As of October 10, 2017: http://www.healthbanking.org/faqs.html

Hembroff, G., "Improving Patient Safety, Health Data Accuracy, and Remote Self-Management of Health Through the Establishment of a Biometric-Based Global UHID," *Studies in Health Technology Informatics*, Vol. 231, 2016, pp. 42–53.

Henry, JaWanna, Yuriy Pylypchuk, Talisha Searcy, and Vaishali Patel, "Adoption of Electronic Health Record Systems Among U.S. Non-Federal Acute Care Hospitals: 2008–2015," *ONC Data Brief*, Vol. 35, 2016.

HHS—*See* U.S. Department of Health and Human Services.

"HIE of One," 2017. As of May 2, 2018: http://hieofone.org/

Hieb, Barry, "A Cost-Effective Method to Create a Universal Healthcare Identifier System," *Electronic Journal of Health Informatics*, Vol. 5, No. 1, 2010, p. e5.

Hieb, Barry, and Elizabeth West, "The Role of Unique Individual Identifiers in Facilitating Healthcare Interoperability," *Journal of Healthcare Information Management*, Vol. 26, No. 2, 2012, pp. 32–37.

Hillestad, Richard, James Bigelow, Anthony Bower, Federico Girosi, Robin Meili, Richard Scoville, and Roger Taylor, "Can Electronic Medical Record Systems Transform Health Care? Potential Health Benefits, Savings, and Costs," *Health Affairs*, Vol. 24, No. 5, 2005, pp. 1103–1117.

Hillestad, Richard, James H. Bigelow, Basit Chaudry, Paul Dreyer, Michael D. Greenberg, Robin C. Meili, M. Susan Ridgely, Jeff Rothenberg, and Roger Taylor, *Identity Crisis: An Examination of the Costs and Benefits of a Unique Patient Identifier for the U.S. Health Care System*, Santa Monica, Calif.: RAND Corporation, MG-753-HLTH, 2008. As of August 7, 2018: http://www.rand.org/pubs/monographs/MG753.html

HIMSS Interoperability & Standards Practices Task Force, *C-CDA Review*, Washington, D.C.: Healthcare Information and Management Systems Society, 2014.

HIPAA—*See* Public Law 104-191.

HITECH—*See* Public Law 111-5.

"HL7 FHIR Argonaut Project," 2018. As of May 2, 2018:
http://argonautwiki.hl7.org/index.php?title=Main_Page

"HL7 Version 2 Product Suite," 2018. As of May 2, 2018:
http://www.hl7.org/implement/standards/product_brief.cfm?product_id=185

"iOS Security," 2018. As of May 8, 2018:
https://www.apple.com/business/docs/iOS_Security_Guide.pdf

Just, B. H., D. Marc, M. Munns, and R. Sandefer, "Why Patient Matching Is a Challenge: Research on Master Patient Index (MPI) Data Discrepancies in Key Identifying Fields," *Perspectives in Health Information Management*, Vol. 13, 2016, p. 1e.

Kohane, Isaac, "Why Apple's Move on Medical Records Marks a Tectonic Shift," 2018. As of February 13, 2018:
http://www.wbur.org/commonhealth/2018/01/26/apple-health-care-data

Landesberg, Martha K., Toby Milgrom Levin, Caroline G. Curtin, and Ori Lev, *Privacy Online: A Report to Congress*, Washington, D.C.: Federal Trade Commission, 1998.
https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf

Lapsia, V., K. Lamb, and W. A. Yasnoff, "Where Should Electronic Records for Patients Be Stored?," *International Journal of Medical Informatics*, Vol. 81, No. 12, December, 2012, pp. 821–827.

Leonard, D. C., A. P. Pons, and S. S. Asfour, "Realization of a Universal Patient Identifier for Electronic Medical Records Through Biometric Technology," *IEEE Transactions on Information Technology in Biomedicine*, Vol. 13, No. 4, July, 2009, pp. 494–500.
http://ieeexplore.ieee.org/document/4534353/

Leventhal, Jeremy C., Jonathan A. Cummins, Peter H. Schwartz, Douglas K. Martin, and William M. Tierney, "Designing a System for Patients Controlling Providers' Access to Their Electronic Health Records: Organizational and Technical Challenges," *Journal of General Internal Medicine*, Vol. 30, No. 1, January 1, 2015, pp. 17–24.

MACRA—*See* Public Law 114-10.

Mandl, K. D., W. W. Simons, W. C. Crawford, and J. M. Abbett, "Indivo: A Personally Controlled Health Record for Health Information Exchange and Communication," *BMC Medical Informatics Decision Making*, Vol. 7, September 12, 2007, p. 25.

Mantravadi, S., "Future of Health Record Banking in Hospital Referral Regions," 2016. As of October 10, 2017:
http://www.ajmc.com/contributor/s-mantravadi/2016/09/future-of-health-record-banking-in-hospital-referral-regions/P-3

Mello, M. M., J. Adler-Milstein, K. L. Ding, and L. Savage, "Legal Barriers to the Growth of Health Information Exchange—Boulders or Pebbles?," *Milbank Quarterly*, Vol. 96, No. 1, March, 2018, pp. 110–143.

Meslin, E. M., S. A. Alpert, A. E. Carroll, J. D. Odell, W. M. Tierney, and P. H. Schwartz, "Giving Patients Granular Control of Personal Health Information: Using an Ethics 'Points To Consider' to Inform Informatics System Designers," *International Journal of Medical Informatics*, Vol. 82, No. 12, December, 2013, pp. 1136–1143.

"MiHIN," 2017. As of May 8, 2018: https://mihin.org/

"Mobile Health App Developers: FTC Best Practices," 2016. As of May 8, 2018: https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-app-developers-ftc-best-practices

Morris, Genevieve, Greg Farnum, Scott Afzal, Carol Robinson, Jan Greene, and Chris Coughlin, *Patient Identification and Matching Final Report*. Baltimore, Md.: Audacious Inquiry, 2014.

Muntz, David, "Thoughts and Recommendations on a National Health Safety Identifier." *Healthcare Informatics*, 2016. As of July 26, 2018: https://www.healthcare-informatics.com/article/thoughts-and-recommendations-national-health-safety-identifier

National Institute of Standards and Technology, *Digital Identity Guidelines*, Washington, D.C.: U.S. Department of Commerce, 2018. https://pages.nist.gov/800-63-3/

NIST—*See* National Institute of Standards and Technology.

Office of Civil Rights. *Individuals' Right Under HIPAA to Access Their Health Information 45 CFR 164.524*, Washington, D.C.: Department of Health and Human Services, 2016. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html#newlyreleasedfaqs

Office of the National Coordinator for Health Information Technology, *Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap*, Washington, D.C.: Office of the National Coordinator for Health Information Technology, 2015. https://www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperability-roadmap-final-version-1.0.pdf

———, *2016 Report to Congress on Health IT Progress*, Washington, D.C.: Department of Health and Human Services, 2016. https://www.healthit.gov/sites/default/files/2016_report_to_congress_on_healthit_progress.pdf

———, *Draft Trusted Exchange Framework*, Washington, D.C.: Office of the National Coordinator for Health Information Technology, 2018a. https://www.healthit.gov/sites/default/files/draft-trusted-exchange-framework.pdf

———, "A User's Guide to Understanding the Draft Trusted Exchange Framework," Washington, D.C.: Office of the National Coordinator for Health Information Technology, 2018b. https://www.healthit.gov/sites/default/files/draft-guide.pdf

———, "What Is HIE?," Washington, D.C.: Office of the National Coordinator for Health Information Technology, 2018c. As of May 8, 2018: https://www.healthit.gov/topic/health-it-and-health-information-exchange-basics/what-hie

ONC—*See* Office of the National Coordinator for Health Information Technology.

Paul, Ron, "Statement of Hon. Ron Paul Before the House SubCommittee on National Economic Growth, National Resources, and Regulatory Affairs: Hearing on National Identifiers 9-17-98," 1998, pp. 137–199.

Pew Research Center, "Mobile Fact Sheet," 2018. http://www.pewinternet.org/fact-sheet/mobile/

Plischke, M., M. Wagner, B. Haarbrandt, M. Rochon, J. Schwartze, E. Tute, T. Bartkiewicz, T. Kleinschmidt, C. Seidel, H. Schuttig, and R. Haux, "The Lower Saxony Bank of Health: Rationale, Principles, Services, Organization and Architectural Framework," *Methods of Information in Medicine,* Vol. 53, No. 2, 2014, pp. 73–81.

Ponemon Institute, *2016 National Patient Misidentification Report*, Traverse City, Mich.: Ponemon Institute LLC, 2016.

PPACA—*See* Public Law 111-148.

Public Law 104-191, Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Public Law 111-5, Health Information Technology for Economic and Clinical Health Act (HITECH), 2009.

Public Law 111-148, Patient Protection and Affordable Care Act of 2010 (PPACA).

Public Law 114-10, Medicare Access and CHIP Reauthorization Act of 2015 (MACRA).

Public Law 114-255, 21st Century Cures Act of 2016 (21st Century Cures).

Rhoades, Harmony, Suzanne L. Wenzel, Eric Rice, Hailey Winetrobe, and Benjamin Henwood, "No Digital Divide? Technology Use Among Homeless Adults," *Journal of Social Distress and the Homeless*, Vol. 26, No. 1, 2017, pp. 73–77.

Rostad, Lillian, and Oystein Nytro, "Personalized Access Control for a Personally Controlled Health Record," *Proceedings of the 2nd ACM workshop on Computer Security Architectures*, Alexandria, Va.: ACM, 2008.

Ryan, Caitlin, "Blockchain Challenge on ONC Tech Lab," 2017. https://oncprojectracking.healthit.gov/wiki/display/TechLabI/Blockchain+Challenge+on+ONC+Tech+Lab

Schwartz, Peter H., Kelly Caine, Sheri A. Alpert, Eric M. Meslin, Aaron E. Carroll, and William M. Tierney, "Patient Preferences in Controlling Access to Their Electronic Health Records: A Prospective Cohort Study in Primary Care," *Journal of General Internal Medicine*, Vol. 30, No. 1, January 1, 2015, pp. 25–30.

The Sequoia Project, *A Framework for Cross-Organizational Patient Identity Management*, 2015. https://sequoiaproject.org/wp-content/uploads/2015/11/The-Sequoia-Project-Framework-for-Patient-Identity-Management.pdf

Sivak, Michael, and Brandon Schoettle, *Recent Decreases in the Proportion of Persons with a Driver's License Across All Age Groups*, Transportation Research Institute, Report No. UMTRI-2016-4, 2016. http://umich.edu/~umtriswt/PDF/UMTRI-2016-4.pdf

Skadden, Arps, Slate, Meagher & Flom LLP and Affiliates, *Privacy & Cybersecurity Update*, New York: Skadden, Arps, Slate, Meagher & Flom LLP and Affiliates, 2018.

Szolovits, Peter, Jon Doyle, William J. Long, Isaac Kohane, and Stephen G Pauker, *Guardian Angel: Patient-Centered Health Information Systems*, Cambridge, MA: Massachusetts Institute of Technology Laboratory for Computer Science, 1994.

Tierney, William M., Sheri A. Alpert, Amy Byrket, Kelly Caine, Jeremy C. Leventhal, Eric M. Meslin, and Peter H. Schwartz, "Provider Responses to Patients Controlling Access to Their Electronic Health Records: A Prospective Cohort Study in Primary Care," *Journal of General Internal Medicine*, Vol. 30, No. 1, January 1, 2015, pp. 31–37.

U.S. Department of Health and Human Services, *Unique Health Identifier for Individuals*, Washington, D.C.: U.S. Department of Health and Human Services, 1998.

Walker, J., E. Pan, D. Johnston, J. Adler-Milstein, D. W. Bates, and B. Middleton, "The Value of Health Care Information Exchange and Interoperability," *Health Affairs*, Vol. Suppl. Web Exclusives, January–June, 2005, pp. w5-10–w15-18.

WEDI—*See* Workgroup for Electronic Data Interchange.

Weitzman, E. R., L. Kaci, and K. D. Mandl, "Acceptability of a Personally Controlled Health Record in a Community-Based Setting: Implications for Policy and Design," *Journal of Medical Internet Research*, Vol. 11, No. 2, April 29, 2009, p. e14.

Weitzman, E. R., L. Kaci, M. Quinn, and K. D. Mandl, "Helping High-Risk Youth Move Through High-Risk Periods: Personally Controlled Health Records for Improving Social and Health Care Transitions," *Journal of Diabetes Science Technology*, Vol. 5, No. 1, January 1, 2011, pp. 47–54.

Weitzman, E. R., S. Kelemen, L. Kaci, and K. D. Mandl, "Willingness to Share Personal Health Record Data for Care Improvement and Public Health: A Survey of Experienced Personal Health Record Users," *BMC Medical Informatics Decision Making*, Vol. 12, May 22, 2012, p. 39.

Workgroup for Electronic Data Interchange, *Virtual Clipboard Initiative Launched to Streamline Patient Intake and Eliminate Wasteful Administrative Processes*, Reston, Va.: Workgroup for Electronic Data Interchange, 2016. https://www.wedi.org/news/press-releases/2014/12/16/Virtual_Clipboard_Initiative_Launched

"Xcertia mHealth App Guidelines," 2017. As of March 2, 2018: http://xcertia.org/

Yasnoff, W. A., and E. H. Shortliffe, "Lessons Learned from a Health Record Bank Start-Up," *Methods for Information Medicine*, Vol. 53, No. 2, 2014, pp. 66–72.

Zech, J., G. Husk, T. Moore, G. J. Kuperman, and J. S. Shapiro, "Identifying Homelessness Using Health Information Exchange Data," *Journal of the American Medical Informatics Association*, Vol. 22, No. 3, May 2015, pp. 682–687.

Zhang, Y., S. Dhileepan, M. Schmidt, and S. Zhong, "Emergency Access for Online Personally Controlled Health Records System," *Informatics for Health Social Care*, Vol. 37, No. 3, September 2012, pp. 190–202.