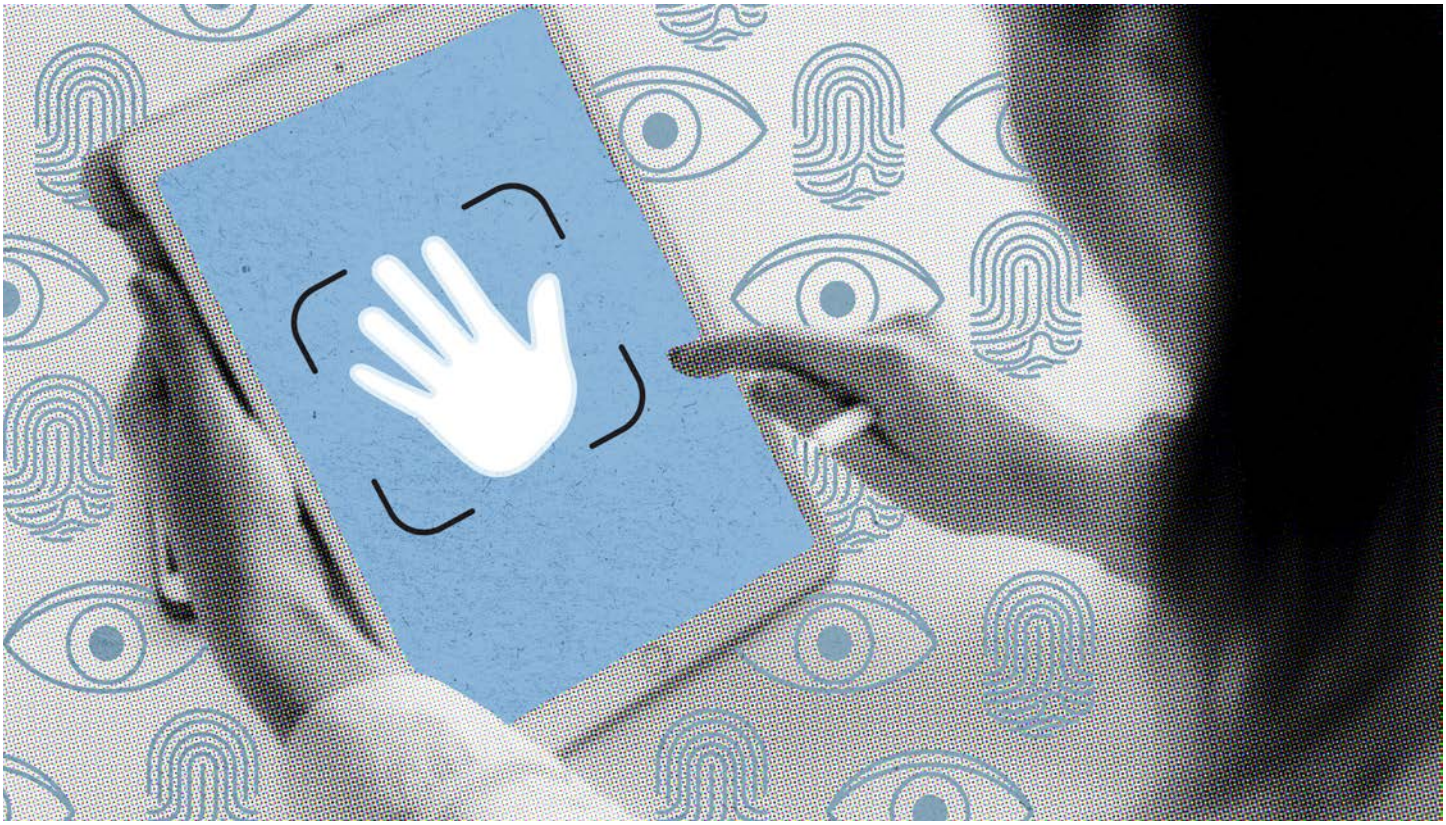


Biometrics Can Help Match Patients to Their Electronic Health Records

Experts discuss how facial images, fingerprints enable health care providers to correctly access and share patient health information

Cover illustration: The Pew Charitable Trusts

Contact: Zach Bernstein, senior communications associate
Email: zbernstein@pewtrusts.org
Project website: pewtrusts.org/healthIT

Contents

The Pew Charitable Trusts

Michael Caudell-Feagan, *executive vice president and chief program officer*
Kil Huh, *senior vice president, government performance*
Kathy Talkington, *director, health programs*

External Reviewers

This report benefited from the insights and expertise of Lucia Savage, chief privacy and regulatory officer, Omada Health Inc., and Laura Schubel, research specialist, MedStar Health Research Institute, National Center for Human Factors in Healthcare. We are also grateful to Ryan Howells, principal, Leavitt Partners, who participated in the research and provided feedback for the report. Although they have reviewed the report, neither they nor their organizations necessarily endorse its findings and conclusions.

Acknowledgments

This report was prepared by Joshua Wenderoff with support from Don Asmonga of Pew's health information technology project. It is based on the work of RTI International, which conducted and summarized the research underlying this document.

We thank current and former Pew colleagues for their contributions: Ben Moscovitch and Molly Murray for initiating and overseeing the research; Sarah Spell, Alan van der Hilst, Matt Mahoney, Maureen Bowers, and Jacqueline Uy for advising on research design and reviewing the results; Zach Bernstein, Sophie Bertazzo, Kimberly Burge, and Tricia Olszewski for their editorial input; Kyra Fryling for helping to prepare the report for publication; Ned Drummond for graphic design; and Shamyra Edmonds for managing its production.

Overview

A patient dies from a heart attack when health care providers mistakenly access another patient's do-not-resuscitate order.[1] A newborn is given another baby's breast milk from a mother infected with hepatitis B.[2] A woman receives a kidney transplant intended for someone else with the same name.[3] These real tragedies resulted from mismatched health records—a common, costly, and preventable problem.

Americans often have multiple electronic health records (EHRs) by different doctor's offices, hospitals, and health systems. Health care providers must match those files to get a complete picture of their patients' health history, but errors in matching records to the correct patient occur up to half of the time.[4] According to a 2012 survey, nearly 1 in 5 hospital chief information officers indicated that patients at their hospitals had been harmed in the previous year because of record mismatches.[5] Each year, these kinds of errors cost the U.S. health care system about $6 billion.[6]

Adding biometrics (such as fingerprints or scans of faces, palms, or irises) to patients' EHRs can enhance matching and improve patient care and satisfaction, reduce health care costs, and boost innovation. Most Americans support using biometrics to enhance health record matching and prefer them over other approaches, such as issuing a unique national identifier to each patient (akin to a Social Security number for health care).[7] However, a variety of logistical, legal, and ethical challenges hinder the use of biometrics. Indeed, there are no known cases of biometrics being used to match EHRs across different health systems in the U.S., and no national technical standards to facilitate the process.

To identify barriers to—and potential solutions for—the use of biometrics to improve patient matching, The Pew Charitable Trusts and RTI International, a nonprofit research institute, conducted a series of 12 interviews between April and July 2020. Then, from October 2020 to March 2021, the researchers held five work group discussions with 29 experts from health systems, insurers, biometric and digital identity technology developers, health information exchange platforms, EHR vendors, patient and privacy advocates, health policy advisers, standards organizations, and the Office of the National Coordinator for Health Information Technology (ONC). (See Appendix B for the methodology and experts who agreed to be named.)

This report, which is based on those interviews and discussions, provides background on patient matching and the potential for biometrics to improve it (Section I) followed by a discussion of the results of the individual interviews and work group discussions (Section II).

The work group participants reached consensus on the following positions:

- Facial imaging is an optimal type of biometrics because it is relatively inexpensive and contactless, and people are already used to having their picture taken for identification purposes. However, the technology raises issues related to privacy, equity, and data security.
- Storing encrypted biometrics on patients' personal devices (such as smartphones) is preferable to storing them in a single national repository or across various health systems' databases. Called "match-on-device," this approach reduces security and privacy risks but can introduce logistical and accessibility-related challenges, especially for patients without a smartphone or broadband internet connection.
- Biometrics should be used alongside demographic data such as address, birthdate, and Social Security number to match patient records; they should not be the sole matching mechanism. (As a result, this report uses the term "biometrics-enhanced patient matching" to describe this hybrid approach.)

- National policies and standards are needed to ensure that different health care and EHR systems can exchange information as easily as possible. Further, biometrics technology should not favor or be based on any particular vendor's proprietary technology, which could limit usability.
- Patients' rights should be at the center of decisions around biometric standards. Federal legislators and regulators should study the extent to which existing privacy regulations apply to biometrics and enact and enforce additional policies as needed to protect patients' biometrics from being misused for data mining, surveillance, or other purposes for which patients do not provide informed consent.

Section I: Background on patient matching and biometrics

Most Americans receive treatment from multiple health care providers; nearly a third of older adults, for example, see at least five different physicians each year.[8] As a result, they have multiple EHRs stored across their providers' systems, each one a puzzle piece that must be matched with other records to reveal a complete medical picture.

Ideally, wherever patients go, their records should be readily available to health care providers. In practice, however, attempts to match these records across different health care settings often fall short.

When health care providers try to access their patients' records—either from within or from outside their own offices, hospitals, or health systems—mismatches occur for a variety of reasons.

- People often have the same personal details. For example, one Houston-area health system alone documented 138,000 cases where two or more patients shared the same birthdate and first and last name.[9]
- Addresses, birthdates, and other data are not formatted consistently. For example, some systems use an MM/DD/YYYY format for dates, while others use a MM/DD/YY format. Even recording "Street" in one record and abbreviating "St." in another can produce a mismatch.
- Data often changes; people move, change their name, or switch phone numbers.
- Health care providers, administrators, and other professionals can enter patient information into health records incorrectly.

Adding biometrics to patients' EHRs and using them alongside other demographic data (such as name, address, birthdate) could improve matching rates for several reasons.

- Fingerprints, faces, palms, irises, and other features are unique to individuals.
- These features change little, if at all, and are inseparable from the patient.
- Many people are already comfortable using biometrics for other purposes—such as opening their smartphones, completing financial transactions, or traveling.

However, several barriers must be overcome before using biometrics nationwide to enhance patient matching.

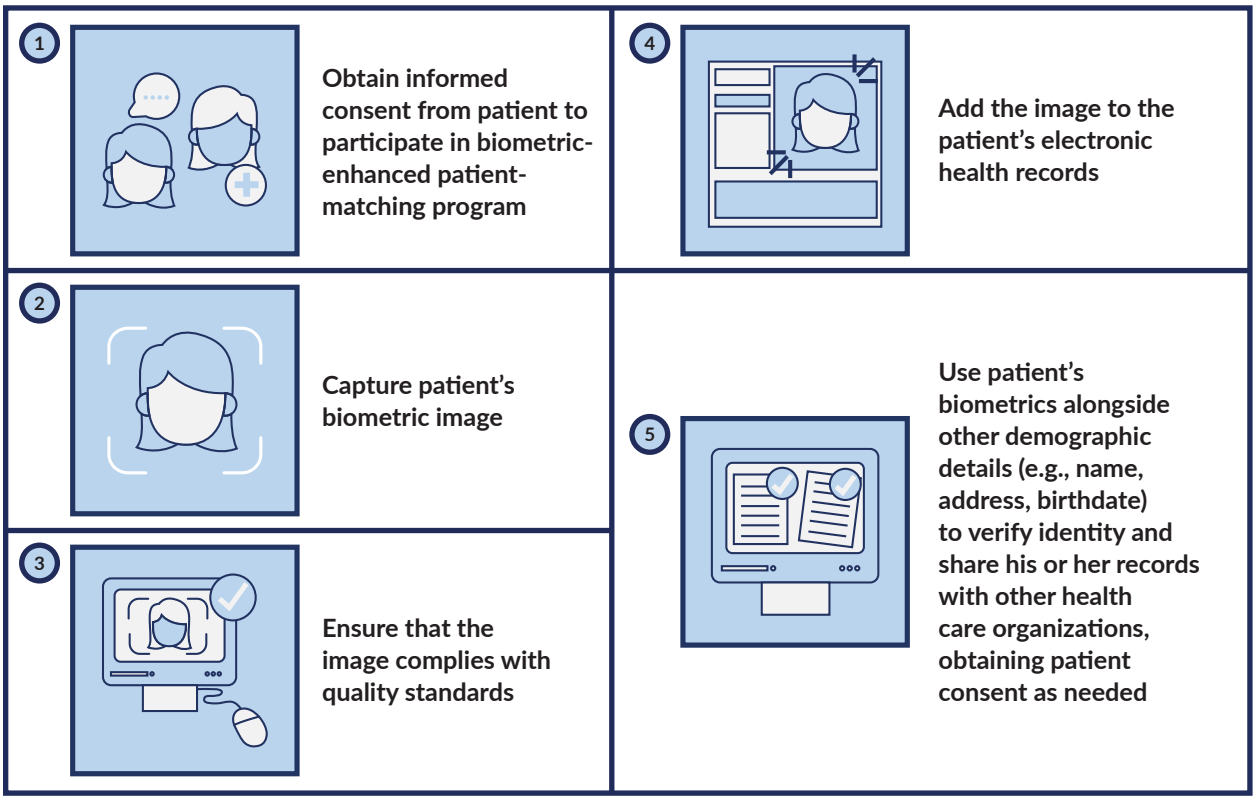
- *Interoperability.* There are hundreds of government-certified EHR products but no national technical standards for capturing biometric images, encrypting biometric data in storage or transmission, or comparing and matching biometrics—all of which are necessary to facilitate the exchange of biometric information between different systems, known as interoperability.[10] Even within the same organization, interoperability is a major issue: According to HIMSS Analytics, an association of health information technology professionals, the average health system uses 16 distinct EHR platforms.[11]
- *Privacy and security.* Because biometrics cannot be changed, any breach of an individual's biometrics would remain for all future use. Existing privacy laws, such as the Health Insurance Portability and Accountability

Act of 1996 (HIPAA), already protect patients' personal information stored and exchanged by "covered entities," including health care organizations. However, additional protections may be needed to explicitly safeguard biometrics stored on patients' personal devices and to ensure that patients can provide informed consent before participating in biometrics-enhanced patient-matching programs. For example, HIPAA does not apply to third-party health and wellness apps unless they are developed for or by covered entities.[12]

- *Feasibility.* Biometrics require investments of time and money in hardware, software, implementation, employee training, patient education, monitoring, maintenance, and support. Although several hospitals have already implemented biometrics to identify patients internally (efforts to improve service and prevent fraud, such as when someone uses another person's identity and insurance coverage to receive treatment), there is no known case of biometrics-enhanced patient matching across different health systems.
- *Equitable access.* Small hospitals, rural health care clinics, stand-alone practices, and other providers may not have the resources to buy biometric technology and hire staff to operate it, or they may be situated in a region with poor internet connectivity. Some biometric solutions require patients to have smartphones, and people earning lower incomes are more likely to experience illness and less likely to own smartphones.[13] In addition, there will always be populations for whom a given type of biometrics does not work. For example, fingerprinting does not work as well for older adults or people with certain skin conditions such as eczema.[14] And facial imaging tends to be less accurate for people with dark complexions due in part to bias in the development of the algorithms.[15]

Figure 1

Basic Biometric Workflow: How Biometric Data Is Captured and Used



Section II: Expert opinions regarding biometrics-enhanced patient matching

Pew and RTI conducted this research in two phases: 12 semistructured individual interviews between April and July 2020 to identify priority areas for consensus and potential models for deeper discussion, followed by five work group sessions between October 2020 and March 2021. Twenty-nine technical, legal, and implementation experts participated in the work group sessions, with most joining at least three meetings, to identify and compare approaches to biometrics-enhanced patient matching. To help establish consensus, researchers used the Delphi Method, a structured communication technique that uses questionnaires to solicit opinions, shares the aggregated results with work group participants, and employs group discussion to move toward consensus. See Appendix B for lists of experts who agreed to be named, individual interview guides, and work group questionnaires.

Among the main consensus points the work group participants reached:

- Biometrics should be used in conjunction with demographic data (for example: names, birthdates, addresses) to improve patient-matching rates. They should not be the sole method of matching.
- Health care organizations will need to educate patients, communicating plainly in the patient's primary language about the benefits and risks of biometrics, and obtain informed consent before asking them to opt in to the collection and use of their images. Health care organizations should also accommodate patients who cannot or do not want to share biometrics, allowing them instead to continue using demographic details to verify patient identity and match records.
- Patient-matching technologies should be nonproprietary and vendor-agnostic to foster as much interoperability as possible.
- Raw biometrics stored in patients' EHRs are protected under HIPAA and should be shared across systems only to enhance patient matching.

The other findings relate to specific approaches and can be categorized by three questions:

1. Which biometrics (fingerprints, faces, palms, irises) are optimal?
2. In what format should they be saved and shared?
3. What is the optimal model for storing and accessing biometrics?

1. Which biometrics are optimal?

The experts weighed the advantages and disadvantages of fingerprints, facial images, palm scans, and iris scans but focused their discussion on the first two options, which they regarded as the most feasible for national implementation in one to three years.

Most work group participants found fingerprints and face scans to be very or moderately feasible, giving face scans a slight edge. Individual interviewees mentioned face scans most often as the optimal type of biometrics because the process is relatively inexpensive, contactless, and familiar to the millions of people who already rely on technology. They noted that palm vein and iris scans were more secure but less feasible than faces and fingerprints because they require more specialized and expensive equipment (such as a camera with near-infrared capabilities).

Table 1

Experts Favor Facial Images Slightly Over Fingerprints

Contactless, inexpensive, and familiar technology is well positioned for widespread use

	Pros	Cons
Fingerprints	• Allow for multiple collection methods (e.g., on-site enrollment, fingerprint scanner on some smartphones) • Collecting 10 prints at enrollment allows for multiple options in the event of injury or other challenges with collecting prints from a single finger • Can be used to differentiate between family members, including twins • The only type of biometrics for which there is already a standard for converting images to templates, which can strengthen privacy • Can be stored and/or shared with other facilities using the existing template from the National Institute of Standards and Technology (NIST), mitigating some security concerns	• Unreliable for use with pediatric and geriatric patients • Need to be collected serially over the course of the patient's life, as fingerprints can change • Cannot be reliably collected remotely because not all phones have a fingerprint reader • Collecting 10 prints may be burdensome • The standard template for fingerprints is designed for verifying that people have asserted their identities accurately, not identifying people who have not asserted their identity; for this latter purpose, vendors often add proprietary data to the standard template, which undermines interoperability • Strong connotations with law enforcement and criminal justice may undermine some patients' willingness to participate • Collecting fingerprints at a health care facility requires dedicated hardware • Require physical contact, increasing risk of spreading infectious diseases • Patients cannot read fingerprints themselves, so they cannot fix discrepancies on their own

Facial scan	• Faces are visible in public and often widely shared on social media, mitigating some privacy concerns* • Many health care facilities already have the technology and an established workflow to collect images of patients at registration • Many EHR systems can already capture and store the image of the patient • Remote enrollment may be easier than fingerprinting as most phones have cameras to collect images of sufficient quality • Sharing a self-taken photograph is a familiar process and could be more acceptable to more individuals • One set of widely used standards for exchanging information between health care organizations (known as HL7) already includes a standard for patient photos • Doctors, nurses, and other staff can read faces to identify patients in person and verify the match	• No national standards for facial image templates • The existing standard for facial images is not designed for biometrics-enhanced patient matching, so quality-related standards may still need to be developed • Strong connotation with law enforcement, criminal justice, and passive surveillance may undermine some patients' willingness to participate • Less reliable for differentiating between twins and other family members • Technology can reflect and perpetuate racial and ethnic inequities • Because faces can change, images would need to be re-collected over time

* Some participants said that facial images need regulatory protection because they are linked to surveillance. Indeed, about half of American adults currently have their facial images in a law enforcement network, often without their knowledge.[16] Moreover, private companies have capitalized on the lack of restrictions on the use of facial images to retrieve billions of photos from the internet for commercial and law enforcement purposes.[17] As a result, participants noted that Congress, federal regulators, and health care organizations have a responsibility to set clear policies that require patients to provide informed consent for the use of their biometrics and restrict that usage to ensure that it is not employed for unapproved purposes, including data mining and surveillance.

2. How should biometrics be formatted?

There are two main options for formatting biometrics: raw image and template.

- Raw images are unprocessed or lightly processed versions of the original captures. Storing and sharing a raw image increases interoperability because proprietary algorithms are not involved, but decreases security in the event of a breach. There are already well-established standards for quality of facial,[18] finger,[19] and iris[20] images. (See Appendix G for a list of these and other relevant standards.)
- Templates are numerical representations of the original biometric images created by mathematical algorithms. For example, a template could store the coordinates of fingerprint patterns or the positioning of facial features. Templates increase security by creating a condensed version of the biometric data abstracted from the original raw image but decrease interoperability because they are often proprietary. There are international standards for creating a template from a fingerprint but not from faces.

Expert participants decided that raw images are less secure but allow for greater interoperability between systems, whereas templates are more secure but less interoperable. On balance, most participants agreed that, to protect patients' privacy and security, health systems should use templates and should not retain or exchange raw images. A chief concern cited: If raw images are breached, they cannot be changed and would remain compromised for future use. However, some participants believed that security benefits of templates were overemphasized; if a standardized template is breached, they asserted, then the impact and security risks are largely the same.

What Are the Privacy and Security Implications of Biometrics-Enhanced Patient Matching?

Before the work group, 19 participants reported their level of concern for risks to the privacy and security of patients and the related risks for providers, which include legal liability, reputational risk, and cost.[21]

Figure 2

Level of Concern for Patient Risk

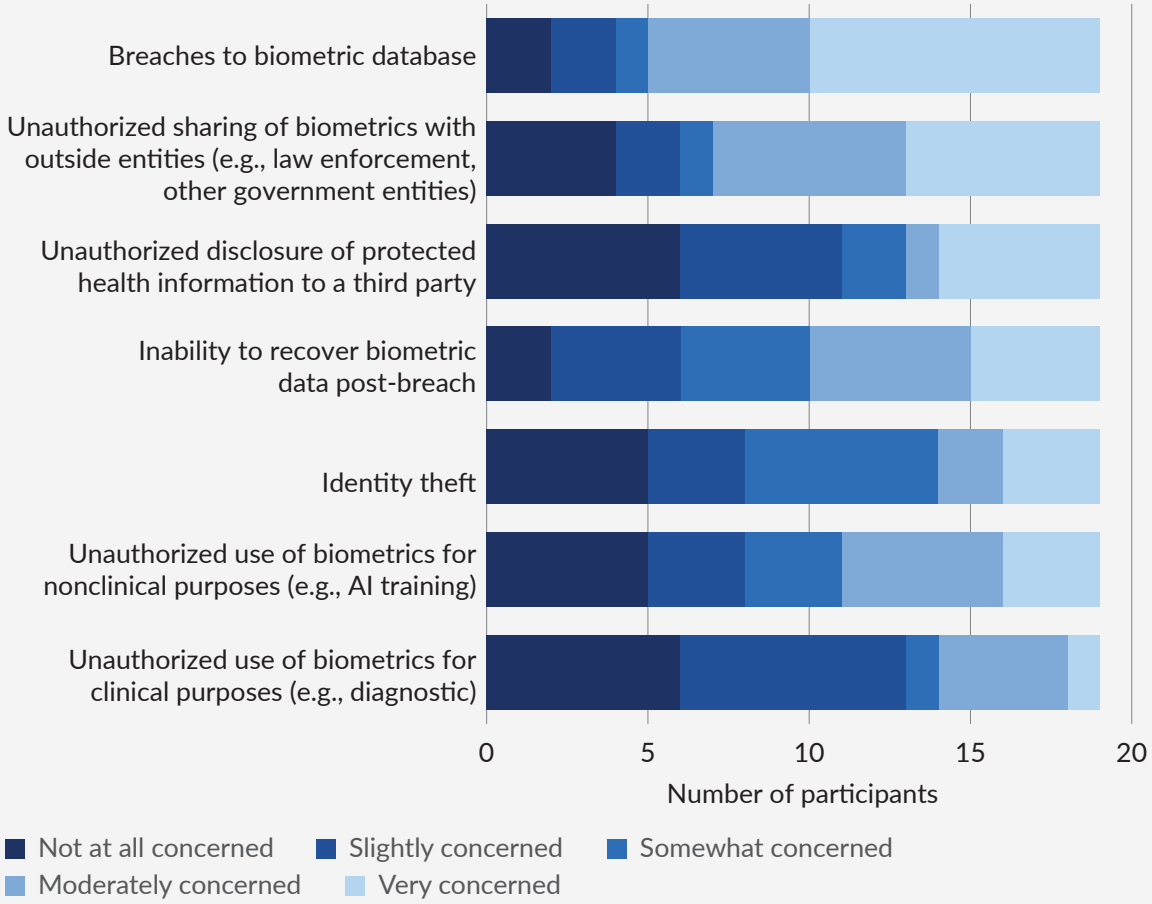
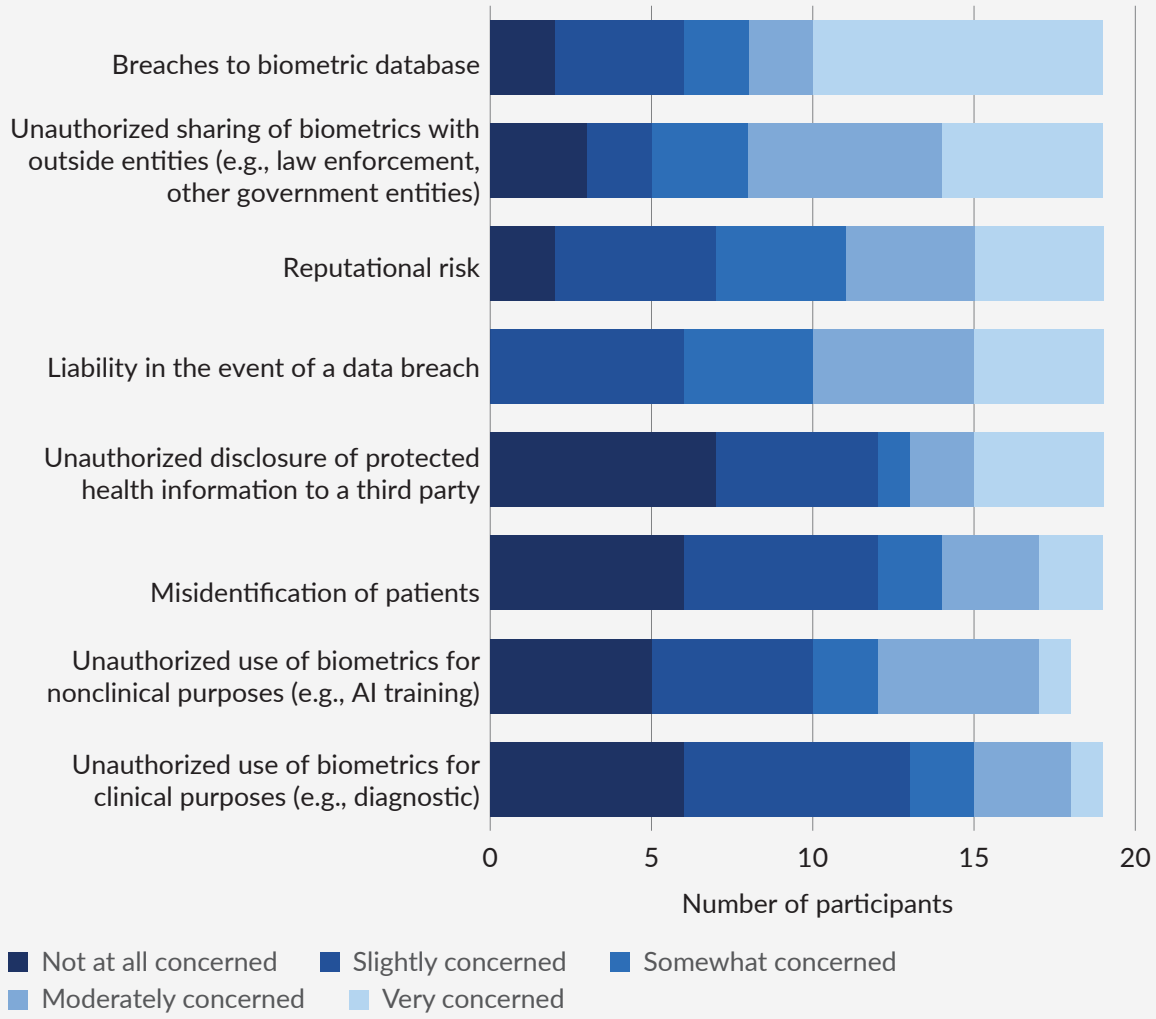


Figure 3

Level of Concern for Provider Risk



Note: One respondent did not respond to the "Unauthorized use of biometrics for nonclinical purposes (e.g., AI training)" question.

3. What is the optimal model for storing and accessing biometrics?

The work group participants considered three models: match-on-device (or MoD), single modality, and multiple modality, all of which are defined below. They agreed that whichever model is employed, biometrics should be used alongside—not in place of—other demographic data (such as name, birthdate, Social Security number) to match patients.

Participants considered principles for each model (see Appendix B2.d for a complete list); below are the principles for which there was majority consensus and no disagreement.

Match-on-device

Definition: Patients use a third-party app on a personal device to capture their biometric data, create an encrypted patient ID, and add it to their records.

Trade-offs: Privacy vs. feasibility and equity

Discussion: Most work group participants preferred MoD over the other two approaches. The primary advantage relates to privacy: Patients use an app on their mobile device to store their biometrics and generate a pair of alphanumeric keys—one private and one public—that enhance security. The biometric data stays on the patient's mobile device, rather than being shared among health care organizations or stored in a centralized database where it can be breached. Some participants believed that raw biometric data (such as a facial image) should be shareable and would not need to be restricted to the patient's device.

MoD also gives patients greater control, because they would play a more hands-on approach in the sharing, storage, and exchange of their biometric data. But this also represents a drawback: Requiring patients to consent to each instance that their health information is shared would inhibit the ready exchange of information that can be important for patient care. Health systems send dozens of queries for single patient records during off-peak hours, often in the middle of the night, which would be unrealistic for patients to respond to. One potential solution would be to collect consent at the time of registration that would cover potential instances in which the public key would be shared and with whom. (Note: One peer reviewer noted that informed consent is not necessarily a significant barrier to MoD because federal regulations allow biometrics in the custody of a "covered entity" under HIPAA—such as hospitals, health care systems, doctor's offices, health plans, and health care clearinghouses—to be shared under many circumstances.)[22] Further discussion of patient consent processes would be an important logistical consideration to moving forward with this model.

HIPAA applies only to covered entities—not to most third-party apps. As a result, patient biometrics that are captured by or stored on an app would not be protected by HIPAA and could be used pursuant to the app's terms of service or end user agreement, which might allow for patient data to be sold commercially or disclosed to government agencies. As a solution, the app developers could be designated as "business associates" of covered entities, which would require the apps to comply with HIPAA. Additionally, policymakers could extend existing regulations, or create new policies, to protect biometrics stored via MoD apps.

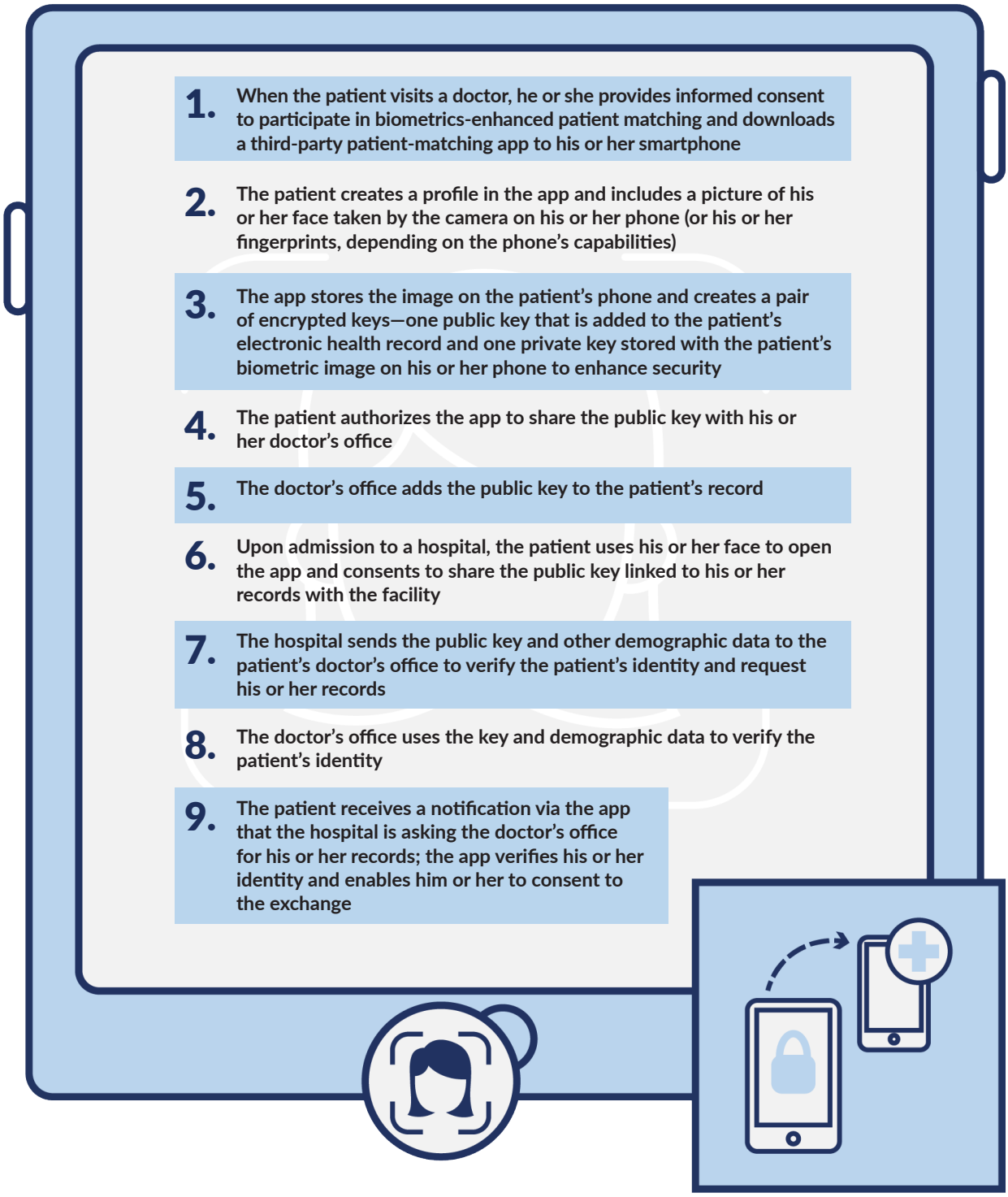
Many experts said that standards such as Fast IDentity Online (FIDO) could be used to facilitate MoD and provide some privacy protections. Because Apple, Google, and Microsoft operating systems and browsers already support FIDO authentication, the standard could speed the development of an interoperable system.[23] Participants also noted that two other organizations—UDAP.org, a publisher of open standards for digital identity verification, and the CARIN Alliance, a multisector association focused on health information exchange—are developing methods to verify digital identities that could support MoD. It is important to note, though, that these standards are being developed for verification, not patient matching.

Work group participants cautioned that MoD could leave behind those patients who lack a smartphone or internet access. Given the correlation between income and health, those who can least afford the technology tend to require more care. Participants expressed that these patients—and those who do not consent to sharing their biometrics—must be accommodated, such as by allowing them to continue using demographic data to match records.

Participants noted that standards-setting organizations, government agencies, health care providers, and other stakeholders must design and adopt standards to avoid the creation of duplicate records. If health care organizations use different third-party apps for MoD, for example, they would need to ensure that those apps still generated the same alphanumeric keys associated with each patient's biometrics.

Figure 4

Use Case for Match-on-Device



Principles: Work group participants reached some consensus on the following principles for MoD:

- MoD should rely only on the exchange of alphanumeric keys; facial images, fingerprints, or other biometrics should be stored locally on the individual's device.
- Patients should opt into this approach by choosing to download the app and agreeing to its terms. Participants noted that hospitals are already using biometrics for purposes other than matching records (for instance, to help staff recognize and identify patients) and allow patients to opt out of biometrics and easily delete images that have already been taken.
- MoD should allow patients to choose whether to use their faces or fingers for the biometrics, accommodating the technology available to them. For example, some smartphones have buttons that enable fingerprint capture, while others can capture only facial images.
- A national organization or government agency should establish technical standards for smartphone apps to facilitate MoD, including collection of biometric data and exchange of an associated key or identifier. Standards for developing these apps would enable multiple apps to be created and used; the solution would not need to be limited to one app.
- MoD should use open standards such as OAuth/OpenID Connect and UDAP (Unified Data Access Profiles) that develop and adhere to a set of best practices to verify patients' identities securely and efficiently.
- When a patient-matching app enrolls a patient, it should use multiple authenticators (such as PINs or verification via text message) so people do not have to re-register if they replace their devices.

Single modality

Definition: All health care organizations adopt and use a single biometric modality (e.g., facial image or fingerprint) to enhance patient matching.

Trade-offs: Interoperability vs. security

Discussion: This approach could foster the greatest level of interoperability, but only if health care organizations adopt national technical standards for capturing, storing, and exchanging biometrics. Additionally, EHR vendors have developed proprietary templates; their continued use would impede data exchange.

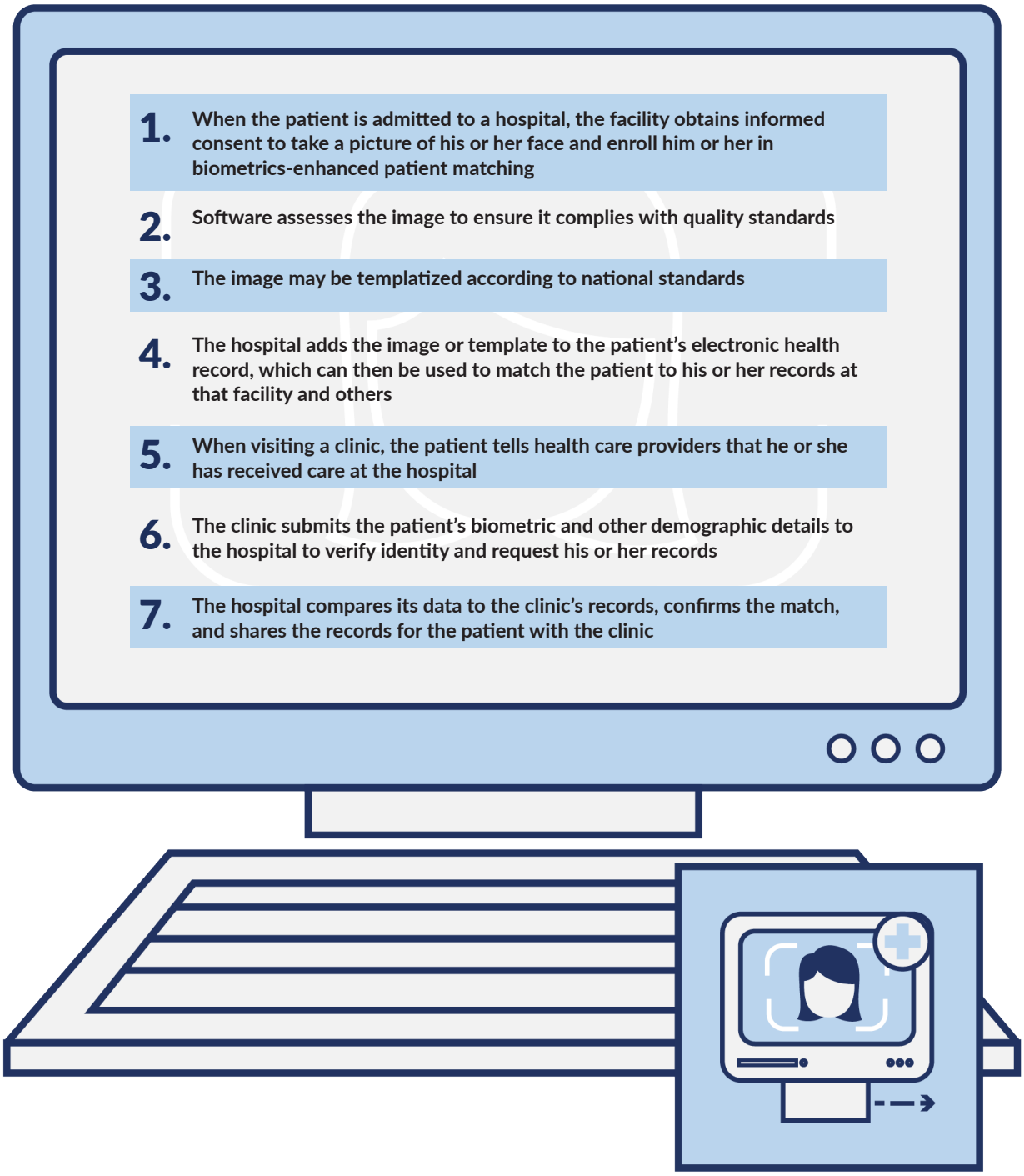
As noted above, the work group participants slightly favored facial images over fingerprints, but they found that using any biometric data exclusively could exacerbate issues of interoperability, security, and equity. If health care systems agree to use the same biometrics, they must also agree to the same format—in other words, raw image or template. Although there is a national standard for "templatizing" fingerprints, there isn't one for facial images. Using raw images could improve interoperability, but that would undermine patient privacy and security. In addition, using a single modality will inevitably exclude certain populations for which the biometric data works poorly (such as fingerprints for older adults, facial images for people with dark skin).

Participants suggested that ONC and the National Institute of Standards and Technology (NIST) work together to create national technical standards to ensure privacy and security when incorporating facial images into health records and as part of health data exchange. They also said that ONC should require EHR vendors to include a technical standard for collecting and exchanging facial images and/or their templates.

See Appendix D for a list of relevant national standards that could help achieve interoperability.

Figure 5

Use Case for Single Modality



Principles: Participants reached consensus on the following principles for a single modality approach:

- Health care facilities should collect patient photos of sufficient quality to facilitate record matching.
- Photo capture should adhere to the NIST's specifications for image composition, including resolution and placement of the head.[24] During the discussion, participants noted that it would be better if health organizations captured the photos rather than accepting patient-submitted photos, which could be poor quality and subject to fraud.
- EHR vendors should enable patient photos to be stored in the EHR as a feature of demographic data, ensuring that they can be used in tandem to enhance patient matching.
- Health care facilities should maintain a human review process to manually adjudicate unmatched records containing biometric samples. This would ensure that biometrics do not fully replace any needed human review, but rather supplement and improve the current matching process. Using faces rather than fingerprints would make it easier for health care providers and administrators to mediate discrepancies.

Multiple modality

Definition: Health care organizations use different biometric modalities (such as fingerprints and facial scans) associated with a single patient to cross-reference the same patient when attempting to validate a match. Such an approach would likely require using a third-party repository, such as a health information exchange, to store biometrics.

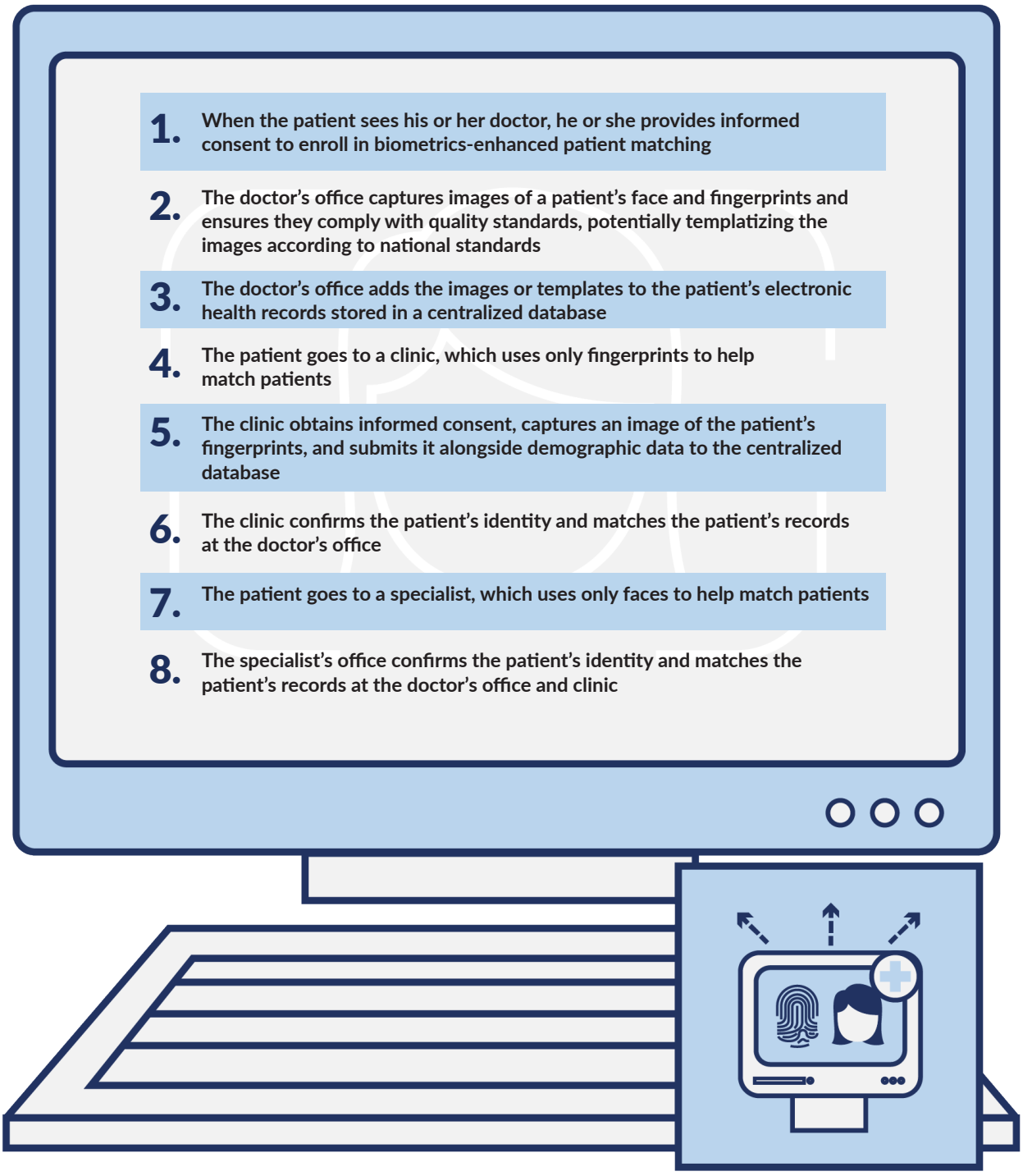
Trade-offs: Flexibility and equity vs. feasibility and security

Discussion: Among its chief benefits, this approach allows health care organizations to choose both their vendor and modality. It also enables patients to use a preferred biometric type if the primary modality does not work for them (for example, fingerprints that are difficult to obtain for older adults). But this complicates the matching process, requiring multiple sets of open standards for the various biometrics and an independent organization to serve as a repository for all health care organizations. Centralizing the data would provide hackers with a one-stop shop to steal patients' personal information.

Given this workflow and the time it would take to build up a repository with enough biometric and other information to measurably improve patient match rates, participants advised that this model is not a priority for near-term implementation. However, this could be a potential model in the next decade, building on a match-on-device or single modality approach.

Figure 6

Use Case for Multiple Modality



Principles: Although stakeholders agreed that an approach in which parties use different biometrics associated with a patient to cross-reference matching would be the least preferred and least feasible, they agreed on some principles for the multiple modality approach if it is pursued:

- Biometrics should be captured at the health care facility using the hardware of the facility's choice or, when providing remote services, by patients using a personal device. This maintains flexibility for health care facilities and accommodates telehealth services.
- Biometric data-collection systems should adhere to NIST specifications for image quality and composition to ensure the data is usable.
- EHR vendors should ensure that multiple biometric modalities can be stored as a feature of patient demographic data.

Figure 7

Summary of Patient-Matching Models

	Pros	Cons
Match-on-device: Patients use a third-party app on a personal device to capture their biometric data, create an encrypted patient ID, and add it to their records	• Stronger security and privacy protections because biometrics are stored on patients' devices • Rather than sharing raw images, health care organizations exchange public keys, which can be changed if they are compromised • Allows for multiple modalities • Patients have more control over the sharing of their biometrics	• Complicated processes could slow care, especially if patients must consent to sharing often • People without smartphones would be left behind
Single modality: All health care organizations adopt and use a single biometric modality (e.g., facial image or fingerprint) to enhance patient matching	• Greater interoperability if all health care organizations agree to use the same biometrics and standards for capturing, templatizing, and sharing it	• A single biometric modality will not work for everyone, which means that some patients would be excluded (e.g., older adults who cannot provide a fingerprint) • If biometric images are breached, they can be compromised for all future use
Multiple modality: Health care organizations use different biometric modalities associated with a single patient to cross-reference the same patient when attempting to validate a match	• Accommodates patients for whom some modalities do not work • Allows health care organizations to choose both their vendor and modality	• Requires a third-party intermediary and multiple standards • Centralized biometrics would be vulnerable to a massive data breach

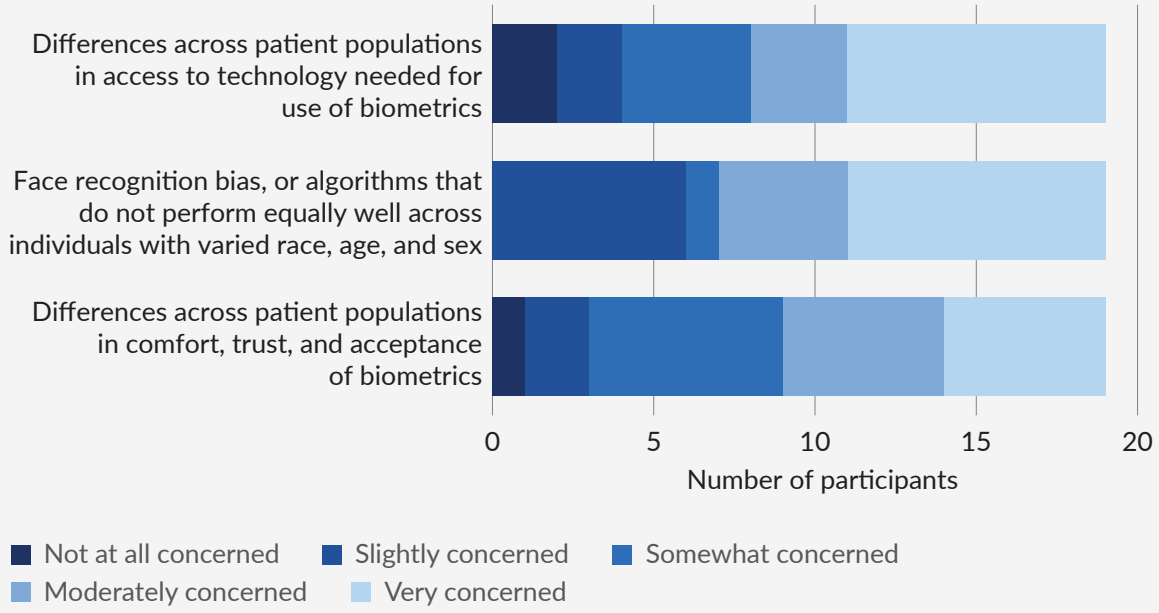
Biometrics and Health Equity

Before the work group, 19 participants rated their level of concern regarding the extent to which patients would have equitable access to biometrics and how consistently the technology would perform for people regardless of their race, ethnicity, age, and sex.[25]

Participants suggested that regulatory agencies, health care organizations, and technology developers should continually assess performance and monitor for instances of bias; update algorithms to remove bias; educate patients to understand and trust the technology; and engage health equity experts alongside technical professionals as they develop and implement biometrics. Additional solutions might be needed to enable patients without smartphones to participate in MoD-based patient-matching systems.

Figure 8

Level of Concern About Patient Equity Issues



Conclusion

Mismatched patient records happen too often and cost too much—and these mistakes are preventable. Federal regulators and lawmakers, standards-setting organizations, health care organizations, technology developers, practitioners, patients, and other stakeholders should consider these findings as they work together to craft secure, interoperable, and equitable solutions. Together, they can advance the use of biometrics to improve patient matching, saving money and lives.

Appendices

Appendix A

Glossary

Term	Definition
Authentication	Confirmation that an individual attempting to access a system possesses a valid authenticator (e.g., a PIN) that is associated with the individual's digital identity.[26]
Biometrics	Detectable biological characteristics of an individual that can be used to extract distinguishing, repeatable features to automate recognition of the individual.[27]
Biometric comparison (or similarity) score	Score that represents the degree to which two biometric presentations (new vs. enrolled) are similar.[28]
Biometric matching	Process that establishes the degree to which two biometric presentations are similar. This is usually displayed in the form at the match score between newly captured biometrics and previously enrolled biometrics.[29]
Digital identity	Unique representation of an individual conducting an online transaction. A digital identity is unique to the context of a digital service being provided but is not necessarily unique in identifying an individual in all situations (i.e., a digital identity is not necessarily tied to an individual's real-life identity).[30]
Duplicate record	An additional (often unintentional) record for a patient with an existing record in a system. [31]
Enrollment	Method through which an individual applies to subscribe to a service provider and the provider of the service verifies the individual's identity.[32]
Fast Identity Online (FIDO)	A standard that uses biometrics and alphanumeric keys to replace password-only logins across multiple websites and apps.[33]
Identity proofing	Process by which a provider collects, validates, and verifies information about an individual person. Identity proofing processes are a subset of what is necessary for enrollment and is conducted by the provider of the service, with cooperation from the individual.[34]
Matching algorithms	Process through which records are matched based on characteristics that are shared between the records.[35]
Modality	The medium or format in which data is captured or collected (e.g., fingerprint, iris scan, etc).[36]
Multifactor authentication	System that requires more than one distinct factor to successfully authenticate an individual.[37]
OAuth	An open-standard authorization protocol.[38]

Term	Definition
OpenID Connect	A standard authentication layer on top of the OAuth protocol.[39]
Patient matching	Comparison of demographic data—such as names and birthdates—that is stored in different records to determine whether those records refer to the same individual.[40]
Private key	The secret part of an asymmetric key pair that is used to digitally sign or decrypt data.[41]
Public key	The public part of an asymmetric key pair that is used to verify signatures or encrypt data.[42]
Raw image	The original image produced during biometric data collection.[43]
Verification	Establishment of a linkage between an individual's claimed identity and the existence of the individual in possession of evidence of the identity.[44]

Appendix B

Participants and Methodology

B1. Individual Interviews

B1.a. Interviewees (titles and affiliations at the time of the interviews)

RTI and Pew collaboratively identified 12 interviewees; nine agreed to be listed below and three did not respond to requests for consent to be named.

Name	Organization	Title
Jeremy Grant	Venable	Managing director of technology business strategy
Ryan Howells	Leavitt Partners; CARIN Alliance	Principal; program manager
Blake Hall	ID.me	Founder & chief executive officer
Michael Petrov	EyeLock	Vice president of technology
Kim Poderis	Aetna	Business project program manager
John Sonnier	Terrebonne General Medical Center	Patient access manager
Lee Tien	Interviewed personally, not representative of his organization (i.e., Electronic Frontier Foundation)	Senior staff attorney
Michael Trader	RightPatient	Co-founder and president
Leslie Kelly Hall	Engaging Patient Strategy	Founder

B1.b. Methodology

Pew and RTI coordinated semistructured individual interviews with 12 key experts between April and July 2020 to explore biometric workflow, technical standards, policy and regulatory issues, feasibility, and privacy. The goal of the interviews was to inform understanding of the resources and knowledge available to build the framework and gain greater understanding of the views of stakeholders across different industries. Knowledge gained from the interviews was used to identify priority areas for building consensus during the work groups and to outline potential candidate models on which additional stakeholders could provide feedback. Interview topics were slightly tailored to match participant expertise, though generally included feasibility, data security, and utilizing existing (data) infrastructure.

B1.c. Individual Questionnaire

Interviews were conducted over Zoom. Questions differed slightly between implementation experts, technical experts, and ethical/legal experts. Given the small number of interviews, manual interview coding was done by two staff members independently.

Section 1. Background

- Can you tell me about your role at [organization]?
- Can you tell me about your work related to [tailor to respondent]?

Section 2. Implementation Experience

[Questions in this section are for interviewees with implementation site perspective]

- What prompted your organization to get started with implementing biometrics?
- What were the steps involved in implementation?
- What vendors did you work with (biometric and other, e.g., EHR, specialty systems reporting systems, health information exchange)? [If use multiple modalities]

Workflow

- How is the biometric data captured and stored?
- What hardware are you using for capturing biometrics (e.g., scanner, iPad, personal device, proprietary device? (e.g., palm vein scanner))?
- What are your organization's policies and practices for retention of biometric data?
- What is the process for patient consent?

Privacy

- What types of security features and practices have been implemented to protect the data and ensure privacy?

Return on Investment and Sustainability

- What are the key costs/other resources associated with implementation of biometrics?
- What has been the return on investment for your organization?
- Is the system that was implemented sustainable for your organization?

Other

- How have patients (and families) responded to the use of biometric data?

Benefits & Lessons Learned

- What was the improvement in matching rates after the implementation of biometrics?
- What are the key lessons learned from your organization's experience with development and implementation of biometrics for patient matching?

Section 3. Workflow

[Questions in this section are for interviewees with technical perspective]

- What biometric modality or modalities do you consider as best suited for health care (e.g., facial recognition, iris scan, palm vein scan, fingerprint)?
- How is this type of biometric data captured? *[Ask for each modality mentioned]*
- Where can this type of biometric data be stored (both the raw data and the template that digitally references features extracted from the human trait captured)? *[Ask for each modality mentioned]*
- How and when should individuals have their biometrics scanned for the first time?
- How should individuals subsequently be linked to records associated with those biometrics?
- What should policies and practices be related to retention of biometric data (e.g., if patient leaves a practice, requests data be removed)?

Section 4. Technical Standards and Infrastructure

[Questions in this section are for interviewees with technical perspective]

- Are there any specific standards you are aware of for the capture, storage, and exchange of biometric data (probe for specific standards)?
- What, if any, standards need to be developed, refined, and incorporated by matching applications to support vendor-agnostic biometrics-based matching in health care?
- What kind of infrastructure is necessary to support the technology, standards, and storage of biometric data?

Section 5. Privacy, Security, and Ethical Considerations

[Questions in this section are for interviewees with ethical/legal perspective]

- How can biometrics data be stored, exchanged, and protected to preserve privacy and inhibit illicit use? For example, what information would two unaffiliated health care organizations exchange about an individual to link records when biometrics are used as part of the process?
- What security features and practices should technology vendors and facilities employ to protect the data and ensure privacy?
- If a biometric image or template is exchanged between organizations, what security features should be implemented to protect the data in transit?
- If an illicit actor obtained the raw biometric data or template, how could they use the information?
- Are specific types of biometrics more secure and preferable for preserving privacy?
- How can policies restricting how biometric data may be used by organizations or legal jurisdictions (i.e., for identification versus authentication) be addressed through a framework?
- What are best practices for obtaining patient consent for use of biometrics?

Section 6. Feasibility

[Questions in this section are for all interviewees]

- What would make a biometrics-reliant national framework for patient matching feasible?
- How could such a framework be deployed?
- What would be the costs/other resources needed for implementing such a framework?
- How can we evaluate and monitor the improvement in patient matching accuracy resulting from deploying biometric technology?

Section 7. Wrap-Up

- Before we wrap up, are there any final thoughts you would like to share on the topics we discussed today?
- Is there anyone else you recommend as critical for us to talk to?

B2. Work Groups

B2.a. Participants (titles and affiliations at the time of the work groups)

Name	Organization	Title
Jeremy Grant	Venable	Managing director of technology business strategy
Gamble Heffernan	HealthVerity	Vice president of product management
Blake Hall	ID.ME	Founder and chief executive officer
Julie Maas	EMR Direct	Founder and chief executive officer
Carmen Smiley	Office of the National Coordinator for Health Information Technology	IT specialist (systems analysis)
Cherie Holmes Henry	NextGen Healthcare	Vice president of government and industry affairs
Ryan Howells	Leavitt Partners; CARIN Alliance	Principal; program manager
Jeremiah Mason	authID.ai	Senior vice president of product management
Hans Buitendijk	Cerner Corporation	Director of interoperability strategy
Michael Trader	RightPatient	Co-founder and president
Lisa Bari	Civitas Networks for Health	Chief executive officer
Daniel Cidon	NextGate Solutions	Chief technology officer
Andrew Gettinger	Dartmouth; previously Office of the National Coordinator for Health Information Technology	Professor emeritus; previously chief clinical officer
Dave Cassel	SAFE Health Systems Inc.	President
Aaron Miri	Baptist Health	Senior vice president, chief digital and information officer
Sharon Muscatell	Strategic Health Information Exchange Collaborative (SHIEC)	Vice president strategy and collaboratives
Julia Skapik	National Association of Community Health Centers (NACHC)	Chief medical information officer
Leslie Kelly Hall	Engaging Patient Strategy	Founder
Luis Maas	EMR Direct	Chief technology officer
Tom Meinert	Imprivata	Product line lead

B2.b. Methodology

Work group participants. Following the interviews, RTI and Pew collaboratively assembled 29 technical, legal, and implementation experts to drive consensus on the three candidate models: single modality, multiple modalities, and match-on-device (MoD). Five of the interviewees participated in the work group. Twenty work group participants agreed to be named (see list B2.a); the others did not respond to requests for consent to be named.

Scoping documents. Prior to convening, participants were provided with a background information document as well as a document outlining the scope of the group. The background document outlined motivations for investigating biometric options for patient matching, and the scope document outlined core objectives of the work group, timeline, scope of activities, and foundational principles, structure, and output of the group.

Baseline questionnaire: Before the first session, the 29 work group members were polled through REDCap, a secure, web-based application for online surveys, on their area of professional involvement, feasibility considerations for differing biometric modalities, risks for patients, risks for providers and health care systems, equity issues, and barriers to using biometrics. Nineteen of the participants completed the baseline questionnaire. Of them, six indicated that they were involved in technical implementation in the health care sector, seven in biometrics and identity management, two in policy and legal applications related to biometrics, one in technical standards, and one in patient engagement advocacy. Two respondents did not indicate their professional involvement. See section B2.c below for the questionnaire.

Additional questionnaires and meetings. The work group convened virtually five times between Oct. 15, 2020, and March 31, 2021. Not all participants attended every session. Pew and RTI used the Delphi Method to build consensus among the experts. The Delphi Method is a structured communication technique that involves using questionnaires to solicit individual opinions, sharing the aggregated results with participants, and employing group discussion to move toward consensus. It is commonly used to synthesize expert thought into frameworks that help move industry practice forward.[45]

Work group members were polled on workflow, privacy, and standards issues for the three candidate models during the sessions they attended. Questionnaires, disseminated through Zoom polling, were used to facilitate discussion around areas of disagreement for each candidate model.

- **Kickoff:** This initial session was used to launch the meeting series and set a baseline for future sessions.
- **Session 2:** This session was used to discuss a single biometric modality model to enhance patient matching.
- **Session 3:** This session was used to seek consensus on considerations for a single modality model and for a multiple modality model implementation. During this session, work group members were polled on topics related to the implementation of a single modality system. See section B2.d, "Single Modality Statements," for the poll.
- **Session 4:** This session was used to continue discussion on a multiple modality model and review considerations for MoD implementation. As part of the baseline questionnaire, work group members were polled on topics related to the implementation of a multiple modality model. Additionally, participants were polled during this session on topics related to implementation of a MoD candidate model. See section B2.d, "Match-on-Device Statements," for the poll.
- **Session 5:** This session was used to continue discussion on considerations for MoD implementation. Work group members were polled during this session on revised statements related to MoD considerations. See section B2.d, "Match-on-Device - Revised Polling," for the poll.
- **Ad hoc meetings:** In situations in which additional input was needed from individual stakeholders, researchers conducted one-on-one meetings to elicit further feedback.

B2.c. Work Group Questionnaire

The stakeholder baseline questionnaire was conducted in REDCap and sent to participants before the initial convening of the work group.

Areas of Experience

- Which of the following categories best describes your area of professional involvement? (Select one answer)
    - Clinical care
    - Technical implementation in health care sector
    - Policy and legal considerations related to biometrics
    - Technical standards
    - Regulatory compliance
    - Biometrics/identity management
    - Other, specify
- Please rate your level of familiarity with each of the following topics. Not at all familiar [1] to Very familiar [5].
    - Electronic health records
    - Biometrics
    - Patient matching
    - Privacy and security of patient information
    - Ethical and legal issues related to use of biometrics for patient matching
    - Policies and regulations related to use of biometrics for patient matching
    - Technical standards for the capture, storage, and exchange or sharing of biometrics
    - Technical implementation of biometric solutions in the health care sector
    - Technical implementation of biometric solutions in other sectors
- In which of the following areas do you have professional experience? (Select all that apply)
    - Design and/or development of biometric solutions
    - Selection and/or procurement of biometric solutions
    - Technical implementation of biometric solutions in the health care sector
    - Technical implementation of biometric solutions in other sectors (specify)
    - Evaluation of biometric solutions
    - Other experience related to biometric solutions (specify)

Feasibility

Pew aims to develop a feasible, actionable framework for biometrics-enhanced patient matching. We are interested in your input on the feasibility of different biometric modalities.

- Please rate how feasible you consider each of the following biometric modalities for patient matching. Not at all feasible [1] to Very feasible [5].
    - Facial recognition
    - Iris scan
    - Palm vein scan
    - Fingerprint
    - Multiple modalities
    - Other (specify)

- What are the reasons you rate [fill biometric] as "Very feasible" for patient matching?
- What are the reasons you rate [fill biometric] as "Not at all feasible" for patient matching?
- Please rate how comfortable you are with the following modalities for patient matching. Not at all comfortable [1] to Very comfortable [5].
    - Facial recognition
    - Iris scan
    - Palm vein scan
    - Fingerprint
- What are the reasons you are "Very comfortable" with [biometric] for patient matching?
- What are the reasons you are "Very uncomfortable" with [biometric] for patient matching?

Potential Risks

Use of biometrics for patient matching may have risks for both patients and for the providers and health care systems. We are interested in your review of different potential risks.

- How concerned are you about the following risks for patients? Not at all concerned [1] to Very concerned [5].
    - Identity theft
    - Bias and discrimination
    - Furthering existing inequities
    - Unauthorized disclosure of protected health information to a third party
    - Unauthorized use of biometrics for clinical purposes (e.g., diagnostic)
    - Unauthorized use of biometrics for nonclinical purposes (e.g., AI training)
    - Unauthorized sharing of biometrics with outside entities (e.g., law enforcement, other government entities)
    - Breaches to biometric database
    - Inability to recover biometric data post-breach
    - Other (specify)
- How concerned are you about the following risks for providers or health care systems? Not at all concerned [1] to Very concerned [5].
    - Misidentification of patients
    - Unauthorized disclosure of protected health information to a third party
    - Unauthorized use of biometrics for clinical purposes (e.g., diagnostic)
    - Unauthorized use of biometrics for nonclinical purposes (e.g., AI training)
    - Unauthorized sharing of biometrics with outside entities (e.g., law enforcement, other government entities)
    - Breaches to biometric database
    - Reputational risk
    - Patient unwillingness to participate
    - Liability in case of data breach, unauthorized use of biometrics
    - Other (specify)
- In what ways (if any) has recent news about use of facial recognition for surveillance influenced how you think about use of this technology for patient matching? [open]

- How concerned are you about the following issues related to equity? Not at all concerned [1] to Very concerned [5].
    - Differences across patient populations in access to technology (e.g., smartphones) needed for use of biometrics
    - Differences across patient populations in comfort, trust, and acceptance of biometrics
    - Face recognition bias, or algorithms that do not perform equally well across individuals with varied race, age, and sex (e.g., NIST Report 8280)
    - Other equity issues
- How can biometrics be used for patient matching in a way that protects patient privacy and supports equity?

Potential Barriers

We are interested in your views about potential barriers to use of biometrics for enhanced patient matching.

- Please rate what you consider to be the barriers to using biometrics for patient matching. Not a significant barrier [1] to Major barrier [5].
    - Cost to health care systems
    - Sustainability
    - Consumer acceptance
    - Health care system acceptance
    - Limited biometrics options currently on the market
    - Workflow challenges within a health care system
    - Workflow challenges across health care systems
    - Privacy concerns
    - Furthering existing inequities
- Why do you consider [fill barriers] to be major barriers to use of biometrics for patient matching?

Foundational Principles

Pew aims to develop a feasible, actionable framework for biometrics-enhanced patient matching. We are interested in your input on foundational principles for the framework.

- Please mark how much you agree with each statement. Strongly disagree [1] to Strongly agree [5].
    - A framework for patient matching should support multiple vendors
    - The framework should not rely on or require any proprietary solutions
    - There should not be a single national database to store biometric data
    - Biometric data, such as raw photographic images, should not be stored centrally
    - If retained, biometric data should not be collocated with other personally identifiable information
    - Only processed biometric templates should be retained and exchanged between health systems
    - Biometric data collected for purposes of patient matching will not be cross-referenced against any third-party databases (e.g., databases used for travel, law enforcement, or social media)
    - Biometric data will be used in conjunction with demographic data for patient matching (i.e., biometric data would not be used as a singular solution for patient matching)
- What other foundational principles should be considered in developing a national framework for biometrics-enhanced patient matching?

Recommendations for Stakeholder Group

[The goal of the stakeholder group is to inform a consensus-driven and standards-based framework for biometrics-enhanced patient matching]

- Please share any additional input and suggestions for the work of the stakeholder group to achieve this goal. [open]

B2.d. Foundational Principles for a Biometrics-Enhanced Patient-Matching System

General Statements

Level of agreement was assessed through REDCap as part of the baseline questionnaire.

- A framework for patient matching must be vendor-agnostic.
- The framework will not rely on or require any proprietary solutions.
  Biometric data collected for purposes of patient matching will not be cross-referenced against any third-party databases.
- Biometric data will be used in conjunction with demographic data for patient matching (i.e., biometric data would not be used as a singular solution for patient matching).
- Biometric data, such as raw photographic images, should not be stored centrally.
- There will not be a single national database to store biometric data.
- Only processed biometric templates should be retained and exchanged between health systems.
- If retained, biometric data should not be collected with other personally identifiable information.

Single Modality Statements

Principles in this section were evaluated using Zoom polling during work group session 3. Options for level of agreement to the statement were "Yes," "No," and "Could agree, with changes."

- Health care facilities should collect patient photos of sufficient quality to facilitate record matching.
- Photo capture should adhere to NIST specifications for image composition, including resolution and placement of the head.
- Health care facilities should provide a plain language "benefit-risk statement" to help patients make their decision to permit the use of biometrics for record matching.
- Health care facilities should seek informed consent from patients and accommodate individuals who choose not to opt-in.
- EHR vendors should ensure that patient photos can be stored in the EHR as a feature of demographic data.
- HL7 should update "patient.photo" demographic data type to reflect NIST image quality specification.
- FHIR [Fast Healthcare Interoperability Resources] should be updated to establish standards for the secure exchange of a patient photo (raw image).
- Record-matching algorithms should be updated to include biometrics as an element.
- Biometric technology vendors should complete and disclose results from the NIST Face Recognition Vendor Test (FRVT) to identify and remediate any known demographic differences and ensure equitable performance across all races/ethnicities.
- ONC should compile and distribute a list of the COTS [commercial off the shelf] devices suitable for both

on-site and remote enrollment that reflect the NIST image standards.

- ONC should include patient photos that meet the NIST image quality specification part of the United States Common Data for Interoperability (USCDI).
- TEFCA [The Trusted Exchange Framework and Common Agreement] should recommend that participating organizations obtain patient photos for record matching.
- A consensus statement that the raw facial image is considered patient demographic data protected under HIPAA and will only be shared across systems for purposes of treatment to enable enhancements in enhance patient matching.
- Health care facilities should establish a human review process to manually adjudicate unmatched records containing biometric samples.

Multiple Modality Statements

The stakeholder multiple modality questionnaire was conducted in REDCap and sent to participants before the initial convening of the work group as part of the baseline questionnaire. Options for level of agreement to the statement were "Yes," "No," and "Could agree, with changes." If "Could agree, with changes" was chosen, participants were asked to expand on potential changes.

- The use of this proposed multiple modality approach would allow health care facilities to use a single type of biometric data of their choice and/or support collection of more than one upon enrollment.
    - What changes would you propose to the phrase above?
- Biometrics should be captured at the health care facility using the scanner of the facility's choice, or— when providing remote services—by patients using a personal device.
    - What changes would you propose to the phrase above?
- Biometric data collection systems should adhere to NIST specifications for image quality and composition.
    - What changes would you propose to the phrase above?
- EHR vendors should ensure that multiple biometric data types (e.g., facial image, fingerprint, iris, other) can be stored as a feature of patient demographic data.
    - What changes would you propose to the phrase above?
- To support a multiple modality approach for record matching, a trusted third party, such as an HIE [health information exchange] or a national network, should accommodate intake, storage, and processing of multiple biometric data types for record matching (alongside other demographic data).
    - What changes would you propose to the phrase above?
- Raw biometric data should be submitted to the trusted third party for record matching to ensure interoperability of the data.
    - What changes would you propose to the phrase above?
- The trusted third party should produce a unique ID for each patient and provide the unique ID back to health care facilities, rather than transmitting or returning any biometric data.
    - What changes would you propose to the phrase above?
- The trusted third party should be capable of asserting a linkage with a single record between two or more biometrics obtained through different sources, through the use of other demographic data.
    - What changes would you propose to the phrase above?

- EHR vendors should ensure that the unique ID generated by the trusted third party can be stored as a separate demographic field.
    - What changes would you propose to the phrase above?
- HL7 FHIR resource patient should include biometric data types for facial image, fingerprint, iris, or other sample, in addition to current patient photo, as well as the unique ID generated by a trusted third party.
    - What changes would you propose to the phrase above?
- ONC should update USCDI to include multiple biometric types for record matching.
    - What changes would you propose to the phrase above?
- Record matching algorithms should be updated to include multiple biometrics as elements.
    - What changes would you propose to the phrase above?
- Please share any other comments or details here. If you would like to share a different model than what was outlined at the beginning of the questionnaire, please do so here as well.

Match-on-Device Statements

Statements in this section were evaluated using Zoom polling during work group session 4. Options for level of agreement to the statement were "Yes," "No," and "Could agree, with changes."

- A "Match-on-Device" approach should be used to enhance patient record matching using individualized tokens.
- Match-on-Device systems should rely only on the exchange of tokens and never transmit biometric data—meaning biometric data (e.g., facial image, fingerprint, other type) is only ever stored locally on the individual's device.
- Match-on-Device systems should accommodate repeated exchange of a persistent token across multiple endpoints, enabling a patient to receive a single token for record matching among multiple providers.
- Health care facilities should provide hardware to enable enrollment for patients without their own device.
- Patients should opt-in to this approach by choosing to download the app and agreeing to its terms; provision remains for those individuals who opt out.
- Match-on-Device systems should accommodate both on-site and remote enrollment with the patient's own device.
- Match-on-Device systems should accommodate use of face or finger, depending on device, to create the token.
- [An organization] should establish standards for how to integrate MoD using a stand-alone smartphone app.
- Match-on-Device systems should accommodate creation of portable tokens to support consumer hardware upgrades (e.g., new smartphone) without forcing re-registration.
- Receiving systems [EHRs, other] should include new field to accommodate token-based identifier.
- USCDI/HL7 demographics should include token-based identifier.

Match-on-Device – Revised Polling

Statements in this section were evaluated using Zoom polling during work group session 5. Options for level of agreement to the statement were "Yes," "No," and "Could agree, with changes."

- Match-on-Device systems should incorporate a trust framework to facilitate sharing identity credentials (e.g., OpenID, UDAP) for adoption by implementers.
- [An organization] should establish standards for smartphone apps to facilitate MoD, including collection of the biometrics and exchange of an associated token or identifier.
- Match-on-Device systems should employ the use of multiple authenticators upon enrollment to accommodate best practices for account recovery or consumer hardware upgrades (e.g., new smartphone) without forcing re-registration.
- Which organization do you think is most appropriate to establish standards for smartphone apps to facilitate MoD, including collection of the biometrics and exchange of an associated token or identifier?

Appendix C

Health Systems Using Biometrics

Organization	Vendor
University of Pittsburgh Medical Center	Verato[46]
Northwell Health	Verato[47]
Intermountain Healthcare	Verato[48]
Healthix	Verato[49]
Chesapeake Regional Information System for our Patients (CRISP)	Verato[50]
San Diego Health Connect (SDHC)	Verato[51]
Harris Health System	Imprivata[52]
Marion General Hospital	Imprivata[53]
Community Hospital Anderson	Imprivata[54]
CoxHealth	Imprivata[55]
St. Joseph Health System	Imprivata[56]
Memorial Healthcare System	Imprivata[57]
Terrebonne General Medical Center	RightPatient[58]
University Health Care System	RightPatient[59]
Novant Health	RightPatient[60]
Archbold Memorial Hospital	RightPatient[61]

Appendix D

Relevant Standards

Standard	Title
ITU-T X.1277	FIDO Universal Authentication Framework (UAF)
ITU-T X.1278	FIDO Client-to-Authenticator Protocol (CTAP)
W3C Web Authentication	FIDO2 Web Authentication (WebAuthn)
IETF RFC 6749	OAuth 2.0
OpenID Connect	OpenID Connect Core
ISO/IEC 19784-4:2011/COR 1:2013	Biometric application programming interface — Part 4: Biometric sensor function provider interface — Technical Corrigendum 1
ISO/IEC 19785-1:2015	Common Biometric Exchange Formats Framework — Part 1: Data element specification
ISO/IEC 19785-1	Common Biometric Exchange Formats Framework — Part 1: Data element specification
ISO/IEC 19785-2:2006	Common Biometric Exchange Formats Framework — Part 2: Procedures for the operation of the Biometric Registration Authority
ISO/IEC 19785-2:2006/AMD 1:2010	Common Biometric Exchange Formats Framework — Part 2: Procedures for the operation of the Biometric Registration Authority — Amendment 1: Additional registrations
ISO/IEC 19785-2	Common Biometric Exchange Formats Framework — Part 2: Biometric registration authority
ISO/IEC 19785-3:2015	Common Biometric Exchange Formats Framework — Part 3: Patron format specifications
ISO/IEC 19785-3	Common Biometric Exchange Formats Framework — Part 3: Patron format specifications
ISO/IEC 19785-4:2010	Common Biometric Exchange Formats Framework — Part 4: Security block format specifications
ISO/IEC 19785-4:2010/COR 1:2013	Common Biometric Exchange Formats Framework — Part 4: Security block format specifications — Technical Corrigendum 1
ISO/IEC 19794-1:2006	Biometric data interchange formats — Part 1: Framework
ISO/IEC 19794-1:2011	Biometric data interchange formats — Part 1: Framework
ISO/IEC 19794-1:2011/AMD 1:2013	Biometric data interchange formats — Part 1: Framework — Amendment 1: Conformance testing methodology
ISO/IEC 19794-1:2011/AMD 2:2015	Biometric data interchange formats — Part 1: Framework — Amendment 2: Framework for XML encoding
ISO/IEC 19794-2:2005	Biometric data interchange formats — Part 2: Finger minutiae data
ISO/IEC 19794-2:2005/AMD 1:2010	Biometric data interchange formats — Part 2: Finger minutiae data — Amendment 1: Detailed description of finger minutiae location, direction, and type
ISO/IEC 19794-2:2005/COR 1:2009	Biometric data interchange formats — Part 2: Finger minutiae data — Technical Corrigendum 1
ISO/IEC 19794-2:2005/AMD 1:2010/ COR 2:2014	Biometric data interchange formats — Part 2: Finger minutiae data — Amendment 1: Detailed description of finger minutiae location, direction, and type — Technical Corrigendum 2
ISO/IEC 19794-2:2011	Biometric data interchange formats — Part 2: Finger minutiae data
ISO/IEC 19794-2:2011/AMD 1:2013	Biometric data interchange formats — Part 2: Finger minutiae data — Amendment 1: Conformance testing methodology and clarification of defects

Standard	Title
ISO/IEC 19794-2:2011/COR 1:2012	Biometric data interchange formats — Part 2: Finger minutiae data — Technical Corrigendum 1
ISO/IEC 19794-2:2011/AMD 2:2015	Biometric data interchange formats — Part 2: Finger minutiae data — Amendment 2: XML encoding and clarification of defects
ISO/IEC 19794-3:2006	Biometric data interchange formats — Part 3: Finger pattern spectral data
ISO/IEC 19794-4:2005	Biometric data interchange formats — Part 4: Finger image data
ISO/IEC 19794-4:2005/COR 1:2011	Biometric data interchange formats — Part 4: Finger image data — Technical Corrigendum 1
ISO/IEC 19794-4:2011	Biometric data interchange formats — Part 4: Finger image data
ISO/IEC 19794-4:2011/AMD 1:2013	Biometric data interchange formats — Part 4: Finger image data — Amendment 1: Conformance testing methodology and clarification of defects
ISO/IEC 19794-4:2011/COR 1:2012	Biometric data interchange formats — Part 4: Finger image data — Technical Corrigendum 1
ISO/IEC 19794-4:2011/AMD 2:2015	Biometric data interchange formats — Part 4: Finger image data — Amendment 2: XML encoding and clarification of defects
ISO/IEC 19794-5:2005	Biometric data interchange formats — Part 5: Face image data
ISO/IEC 19794-5:2011	Biometric data interchange formats — Part 5: Face image data
ISO/IEC 19794-5:2011/AMD 1:2014	Biometric data interchange formats — Part 5: Face image data — Amendment 1: Conformance testing methodology and clarification of defects
ISO/IEC 19794-5:2011/AMD 2:2015/ COR 1:2016	Biometric data interchange formats — Part 5: Face image data — Amendment 2: XML encoding and clarification of defects — Technical Corrigendum 1
ISO/IEC 19794-5:2011/AMD 2:2015	Biometric data interchange formats — Part 5: Face image data — Amendment 2: XML encoding and clarification of defects
ISO/IEC 19794-6:2005	Biometric data interchange formats — Part 6: Iris image data
ISO/IEC 19794-6:2011	Biometric data interchange formats — Part 6: Iris image data
ISO/IEC 19794-6:2011/AMD 1:2015	Biometric data interchange formats — Part 6: Iris image data — Amendment 1: Conformance testing methodology and clarification of defects
ISO/IEC 19794-6:2011/COR 1:2012	Biometric data interchange formats — Part 6: Iris image data — Technical Corrigendum 1
ISO/IEC 19794-6:2011/AMD 2:2016	Biometric data interchange formats — Part 6: Iris image data — Amendment 2: XML encoding and clarification of defects
ISO/IEC 19794-7:2007	Biometric data interchange formats — Part 7: Signature/sign time series data
ISO/IEC 19794-7:2007/COR 1:2009	Biometric data interchange formats — Part 7: Signature/sign time series data — Technical Corrigendum 1
ISO/IEC 19794-7:2014	Biometric data interchange formats — Part 7: Signature/sign time series data
ISO/IEC 19794-7:2014/AMD 1:2015	Biometric data interchange formats — Part 7: Signature/sign time series data — Amendment 1: XML encoding
ISO/IEC DIS 19794-7	Biometric data interchange formats — Part 7: Signature/sign time series data
ISO/IEC 19794-8:2006	Biometric data interchange formats — Part 8: Finger pattern skeletal data
ISO/IEC 19794-8:2006/COR 1:2011	Biometric data interchange formats — Part 8: Finger pattern skeletal data — Technical Corrigendum 1
ISO/IEC 19794-8:2011	Biometric data interchange formats — Part 8: Finger pattern skeletal data
ISO/IEC 19794-8:2011/AMD 1:2014	Biometric data interchange formats — Part 8: Finger pattern skeletal data — Amendment 1: Conformance testing methodology
ISO/IEC 19794-8:2011/COR 1:2012	Biometric data interchange formats — Part 8: Finger pattern skeletal data — Technical Corrigendum 1
ISO/IEC 19794-9:2007	Biometric data interchange formats — Part 9: Vascular image data

Standard	Title
ISO/IEC 19794-9:2011	Biometric data interchange formats — Part 9: Vascular image data
ISO/IEC 19794-9:2011/AMD 1:2013	Biometric data interchange formats — Part 9: Vascular image data — Amendment 1: Conformance testing methodology
ISO/IEC 19794-9:2011/COR 1:2012	Biometric data interchange formats — Part 9: Vascular image data — Technical Corrigendum 1
ISO/IEC 19794-9:2011/AMD 2:2015	Biometric data interchange formats — Part 9: Vascular image data — Amendment 2: XML Encoding and clarification of defects
ISO/IEC 19794-10:2007	Biometric data interchange formats — Part 10: Hand geometry silhouette data
ISO/IEC 19794-11:2013	Biometric data interchange formats — Part 11: Signature/sign processed dynamic data
ISO/IEC 19794-11:2013/AMD 1:2014	Biometric data interchange formats — Part 11: Signature/sign processed dynamic data — Amendment 1: Conformance test assertions
ISO/IEC 19794-13:2018	Biometric data interchange formats — Part 13: Voice data
ISO/IEC 19794-15:2017	Biometric data interchange format — Part 15: Palm crease image data
ISO/IEC 19795-1:2006	Biometric performance testing and reporting — Part 1: Principles and framework
ISO/IEC 19795-2:2007	Biometric performance testing and reporting — Part 2: Testing methodologies for technology and scenario evaluation
ISO/IEC 19795-2:2007/AMD 1:2015	Biometric performance testing and reporting — Part 2: Testing methodologies for technology and scenario evaluation — Amendment 1: Testing of multimodal biometric implementations
ISO/IEC TR 19795-3:2007	Biometric performance testing and reporting — Part 3: Modality-specific testing
ISO/IEC 19795-4:2008	Biometric performance testing and reporting — Part 4: Interoperability performance testing
ISO/IEC 19795-5:2011	Biometric performance testing and reporting — Part 5: Access control scenario and grading scheme
ISO/IEC 19795-6:2012	Biometric performance testing and reporting — Part 6: Testing methodologies for operational evaluation
ISO/IEC 19795-7:2011	Biometric performance testing and reporting — Part 7: Testing of on-card biometric comparison algorithms
ISO/IEC TS 19795-9:2019	Biometric performance testing and reporting — Part 9: Testing on mobile devices
ISO/IEC CD TR 21421	Cross jurisdictional and societal aspects of implementation of biometric technologies — Biometrics and elderly people
ISO/IEC CD TR 21421	Cross jurisdictional and societal aspects of implementation of biometric technologies — Biometrics and identity management for major incident response
ISO/IEC 24708:2008	Biometrics — BioAPI Interworking Protocol
ISO/IEC 24709-1:2017	Conformance testing for the biometric application programming interface (BioAPI) — Part 1: Methods and procedures
ISO/IEC 24709-2:2007	Conformance testing for the biometric application programming interface (BioAPI) — Part 2: Test assertions for biometric service providers
ISO/IEC 24709-3:2011	Conformance testing for the biometric application programming interface (BioAPI) — Part 3: Test assertions for BioAPI frameworks
ISO/IEC 24713-1:2008	Biometric profiles for interoperability and data interchange — Part 1: Overview of biometric systems and biometric profiles
ISO/IEC TR 24722:2015	Biometrics — Multimodal and other multibiometric fusion
ISO/IEC WD 24741	Biometrics — Overview and application
ISO/IEC TR 24741:2018	Biometrics — Overview and application

Standard	Title
ISO/IEC 24761:2019	Security techniques — Authentication context for biometrics
ISO/IEC 24779-1:2016	Cross-jurisdictional and societal aspects of implementation of biometric technologies — Pictograms, icons, and symbols for use with biometric systems — Part 1: General principles
ISO/IEC 24779-4:2017	Cross-jurisdictional and societal aspects of implementation of biometric technologies — Pictograms, icons, and symbols for use with biometric systems — Part 4: Fingerprint applications
ISO/IEC 24779-5:2020	Cross-jurisdictional and societal aspects of implementation of biometric technologies — Pictograms, icons, and symbols for use with biometric systems — Part 5: Face applications
ISO/IEC 29109-1:2009	Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 1: Generalized conformance testing methodology
ISO/IEC 29109-1:2009/COR 1:2010	Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 1: Generalized conformance testing methodology — Technical Corrigendum 1
ISO/IEC 29109-2:2010	Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 2: Finger minutiae data
ISO/IEC 29109-4:2010	Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 4: Finger image data
ISO/IEC 29109-4:2010/COR 1:2011	Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 4: Finger image data — Technical Corrigendum 1
ISO/IEC 29109-5:2019	Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 5: Face image data
ISO/IEC 29109-6:2011	Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 6: Iris image data
ISO/IEC 29109-7:2011	Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 7: Signature/sign time series data
ISO/IEC 29109-8:2011	Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 8: Finger pattern skeletal data
ISO/IEC 29109-10:2010	Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 10: Hand geometry silhouette data
ISO/IEC 29120-1:2015	Machine readable test data for biometric testing and reporting — Part 1: Test reports
ISO/IEC CD 29120-1.2	Machine readable test data for biometric testing and reporting — Part 1: Test reports
ISO/IEC 29141:2009	Biometrics — Tenprint capture using biometric application programming interface (BioAPI)
ISO/IEC TR 29144:2014	Biometrics — The use of biometric technology in commercial Identity Management applications and processes
ISO/IEC TR 29156:2015	Guidance for specifying performance requirements to meet security and usability needs in applications using biometrics
ISO/IEC 29159-1:2010	Biometric calibration, augmentation, and fusion data — Part 1: Fusion information format
ISO/IEC 29164:2011	Biometrics — Embedded BioAPI
ISO/IEC TR 29189:2015	Biometrics — Evaluation of examiner-assisted biometric applications
ISO/IEC TR 29194:2015	Biometrics — Guide on designing accessible and inclusive biometric systems
ISO/IEC TR 29196:2018	Guidance for biometric enrollment

Standard	Title
ISO/IEC TR 29198:2013	Biometrics — Characterization and measurement of difficulty for fingerprint databases for technology evaluation
ISO/IEC 29794-1:2016	Biometric sample quality — Part 1: Framework
ISO/IEC 29794-4:2017	Biometric sample quality — Part 4: Finger image data
ISO/IEC WD 29794-5	Biometric sample quality — Part 5: Face image data
ISO/IEC TR 29794-5:2010	Biometric sample quality — Part 5: Face image data
ISO/IEC 29794-6:2015	Biometric sample quality — Part 6: Iris image data
ISO/IEC 30106-1:2016	Object oriented BioAPI — Part 1: Architecture
ISO/IEC 30106-1:2016/AMD 1:2019	Object oriented BioAPI — Part 1: Architecture — Amendment 1: Additional specifications and conformance statements
ISO/IEC 30107-1:2016	Biometric presentation attack detection — Part 1: Framework
ISO/IEC 30107-2:2017	Biometric presentation attack detection — Part 2: Data formats
ISO/IEC 30107-3:2017	Biometric presentation attack detection — Part 3: Testing and reporting
ISO/IEC WD 30107-3	Biometric presentation attack detection — Part 3: Testing and reporting
ISO/IEC 30107-4:2020	Biometric presentation attack detection — Part 4: Profile for testing of mobile devices
ISO/IEC 30108-1:2015	Biometric Identity Assurance Services — Part 1: BIAS services
ISO/IEC TR 30110:2015	Cross jurisdictional and societal aspects of implementation of biometric technologies — Biometrics and children
ISO/IEC TR 30117:2014	Guide to on-card biometric comparison standards and applications
ISO/IEC CD TR 30117	Guide to standards and applications for the integration of biometrics and ICC
ISO/IEC TR 30125:2016	Biometrics used with mobile devices
ISO/IEC 30136:2018	Performance testing of biometric template protection schemes
ISO/IEC 30137-1:2019	Use of biometrics in video surveillance systems — Part 1: System design and specification
ISO/IEC DIS 30137-4	Use of biometrics in video surveillance systems — Part 4: Ground truth and video annotation procedure
ISO/IEC 39794-1:2019	Extensible biometric data interchange formats — Part 1: Framework
ISO/IEC 39794-4:2019	Extensible biometric data interchange formats — Part 4: Finger image data
ISO/IEC 39794-5:2019	Extensible biometric data interchange formats — Part 5: Face image data
ISO/IEC DIS 39794-6	Extensible biometric data interchange formats — Part 6: Iris image data
ISO/IEC 17922:2017	Telebiometric authentication framework using biometric hardware security module
ISO/IEC 19792:2009	Security evaluation of biometrics
ISO/IEC CD 24745.2	Security techniques — Biometric information protection
C-CDA - 2	Consolidated Clinical Document Architecture 2
NCPDP X12	National Council for Prescription Drug Programs X12/005010X22A1 Health Care Claim Payment/Advice

Endnotes

1 ECRI Institute, "ECRI Institute PSO Deep Dive: Patient Identification (Volume 1)" (2016), https://assets.ecri.org/PDF/Deep-Dives/Deep-Dive-Patient-ID-Exec-Summary.pdf.

2 Ibid.

3 C. National Research et al., "The National Academies Collection: Reports Funded by National Institutes of Health," in *Preventing Mental, Emotional, and Behavioral Disorders Among Young People: Progress and Possibilities*, eds. M.E. O'Connell, T. Boat, and K.E. Warner (Washington, D.C.: National Academies Press (US) 2009).

4 The Pew Charitable Trusts, "Health Care Can Learn From Global Use of Biometrics" (2020), https://www.pewtrusts.org/-/media/assets/2020/11/healthcarebiometrics.pdf.

5 College of Healthcare Information Management Executives (CHIME), "Summary of CHIME Survey on Patient Data-Matching" (May 16, 2012), https://chimecentral.org/wp-content/uploads/2014/11/Summary_of_CHIME_Survey_on_Patient_Data.pdf.

6 Black Book Market Research, "Improving Provider Interoperability Congruently Increasing Patient Record Error Rates, Black Book Survey," news release, April 12, 2018, https://blackbookmarketresearch.newswire.com/news/improving-provider-interoperability-congruently-increasing-patient-20426295.

7 B. Moscovitch, "Americans Want Federal Government to Make Sharing Electronic Health Data Easier," The Pew Charitable Trusts, Sept. 16, 2020, https://www.pewtrusts.org/en/research-and-analysis/articles/2020/09/16/americans-want-federal-government-to-make-sharing-electronic-health-data-easier.

8 A. Norton, "Almost 1 in 3 U.S. Seniors Now Sees at Least 5 Doctors Per Year," *HealthDay*, Nov. 2, 2021, https://consumer.healthday.com/11-2-almost-1-in-3-u-s-seniors-now-see-at-least-5-doctors-per-year-2655382216.html.

9 Advisory Board, "Harris Health System Has 500+ Maria Garcias—With the Same Birthday. Here's How It Keeps Them Straight," Feb. 20, 2019, https://www.advisory.com/daily-briefing/2019/02/20/biometrics.

10 M. Reisman, "EHRs: The Challenge of Making Electronic Data Usable and Interoperable," *P&T* 42, no. 9 (2017): 572-75, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5565131/.

11 T. Sullivan, "Why EHR Data Interoperability Is Such a Mess in 3 Charts," Healthcare IT News, accessed June 21, 2022, https://www.healthcareitnews.com/news/why-ehr-data-interoperability-such-mess-3-charts.

12 Office for Civil Rights, "The Access Right, Health Apps, & APIs," HHS, accessed June 21, 2022, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access-right-health-apps-apis/index.html.

13 D. Khullar and D.A. Chokshi, "Health, Income, & Poverty: Where We Are & What Could Help," *Health Affairs Health Policy Brief* (2018), https://www.healthaffairs.org/do/10.1377/hpb20180817.901935/; Centers for Medicare & Medicaid Services, "Medicaid Health Homes: Spa Overview" (2021), https://www.medicaid.gov/state-resource-center/medicaid-state-technical-assistance/health-home-information-resource-center/downloads/hh-spa-overview.pdf.

14 N. Sarfraz, "Adermatoglyphia: Barriers to Biometric Identification and the Need for a Standardized Alternative," *Cureus* 11, no. 2 (2019): e4040, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6456356/.

15 A. Najibi, "Racial Discrimination in Face Recognition Technology," *Science in the News* (blog), Harvard University Graduate School of Arts and Sciences, Oct. 24, 2020, https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/?msclkid=4c6ad1f3cfaa11ecbc00b86c9384a20d.

16 C. Garvie, A. Bedoya, and J. Frankle, "The Perpetual Line-Up: Unregulated Police Face Recognition in America" (Georgetown Law Center on Privacy and Technology, 2016).

17 K. Hill, "The Secretive Company That Might End Privacy as We Know It," *The New York Times*, Nov. 2, 2021, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html?searchResultPosition=1.

18 International Organization for Standardization, "ISO/IEC TR 29794-5:2010 Information Technology, Biometric Sample Quality—Part 5: Face Image Data," accessed May 9, 2022, https://www.iso.org/standard/50912.html.

19 International Organization for Standardization, "ISO/IEC 29794-4:2017 Information Technology, Biometric Sample Quality—Part 4: Finger Image Data," accessed May 9, 2022, https://www.iso.org/standard/62791.html.

20 International Organization for Standardization, "ISO/IEC 29794-6:2015 Information Technology, Biometric Sample Quality—Part 6: Iris Image Data," accessed May 9, 2022, https://www.iso.org/standard/54066.html.

21 A.H. Seh et al., "Healthcare Data Breaches: Insights and Implications," *Healthcare* (Basel) 8, no. 2 (2020), https://www.ncbi.nlm.nih.gov/pubmed/32414183.

22 United States, Uses and Disclosures to Carry Out Treatment, Payment, or Health Care Operations, 45 CFR § 164.506 (2013), https://www.law.cornell.edu/cfr/text/45/164.506; H. Journal, "What Is Considered PHI under HIPAA?," accessed May 12, 2022, https://www.hipaajournal.com/considered-phi-hipaa/.

23 The FIDO Alliance, "How FIDO Works," accessed May 9, 2022, https://fidoalliance.org/how-fido-works/.

24 R.M. McCabe and E.M. Newton, "NIST Special Publication 500-271: American National Standard for Information Systems—Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information – Part 1" (NIST, 2007), https://www.nist.gov/system/files/documents/itl/ansi/Approved-Std-20070427-2.pdf.

25 Najibi, "Racial Discrimination in Face Recognition Technology."

26 P.A. Grassi, M.E. Garcia, and J.L. Fenton, "NIST Special Publication 800-63 Revision 3: Digital Identity Guidelines" (National Institute of Standards and Technology, 2017), https://pages.nist.gov/800-63-3/sp800-63-3.html.

27 S.Z. Li and A. Jain, *Encylopedia of Biometrics* (New York: Springer Science & Business Media, 2009), https://books.google.com/books?id=0bQbOYVULQcC&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false.

28 Ibid.

29 B.V.K. Vijaya Kumar, "Biometric Matching," in *Encyclopedia of Cryptography and Security*, eds. H.C.A. van Tilborg and S. Jajodia (Boston: Springer U.S., 2011), https://doi.org/10.1007/978-1-4419-5906-5_726.

30 The Pew Charitable Trusts, "Standardized Demographic Data Improve Patient Matching in Electronic Health Records" (2019), https://www.pewtrusts.org/en/research-and-analysis/issue-briefs/2019/09/standardized-demographic-data-improve-patient-matching-in-electronic-health-records.

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

32 P.A. Grassi, M.E. Garcia, and J.L. Fenton, "NIST Special Publication 800-63: Digital Identity Guidelines" (National Institute of Standards and Technology, 2017), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

33 The FIDO Alliance, "How FIDO Works."

34 Grassi, Garcia, and Fenton, "NIST Special Publication 800-63."

35 T. Dunstone and N. Yager, "Biometric Matching Basics," in *Biometric System and Data Analysis: Design, Evaluation, and Data Mining*, (Boston: Springer U.S., 2009), https://doi.org/10.1007/978-0-387-77627-9_2.

36 Li and Jain, *Encylopedia of Biometrics*.

37 Grassi, Garcia, and Fenton, "NIST Special Publication 800-63."

38 D. Hardt, "The OAuth 2.0 Authorization Framework," Internet Engineering Task Force, accessed May 12, 2022, https://datatracker.ietf.org/doc/html/rfc6749.

39 OpenID, "What Is OpenID Connect?" accessed May 9, 2022, https://openid.net/connect/.

40 The Pew Charitable Trusts, "Standardized Demographic Data Improve Patient Matching in Electronic Health Records."

41 Grassi, Garcia, and Fenton, "NIST Special Publication 800-63."

42 Ibid.

43 Library of Congress, "Sustainability of Digital Formats—Camera Raw Formats (Group Description)," accessed May 12, 2022, https://www.loc.gov/preservation/digital/formats/fdd/fdd000241.shtml.

44 P.A. Grassi et al., "NIST Special Publication 800-63a: Digital Identity Guidelines Enrollment and Identity Proofing Requirements" (National Institute of Standards and Technology, 2017), https://pages.nist.gov/800-63-3/sp800-63a.html.

45 C. Okoli and S.D. Pawlowski, "The Delphi Method as a Research Tool: An Example, Design Considerations and Applications," *Information & Management* 42, no. 1 (2004): 15-29, https://www.sciencedirect.com/science/article/pii/S0378720603001794.

46 Verato, "The Pew Charitable Trusts Highlights Referential Matching as One of Four Opportunities to Improve Patient Matching in the Exchange of Health Information," news release, Oct. 2, 2018, https://verato.com/news/the-pew-charitable-trusts-highlights-referential-matching-as-one-of-four-opportunities-to-improve-patient-matching-in-the-exchange-of-health-information/.

47 Ibid.

48 Ibid.

49 Ibid.

50 Ibid.

51 Ibid.

52 Advisory Board, "Harris Health System Has 500+ Maria Garcias."

53 Imprivata, "Imprivata PatientSecure Technology Bolsters Patient Safety Inititiatives at Marion General Hospital," accessed May 9, 2022, https://www.imprivata.com/resources/video/imprivata-patientsecure-technology-bolsters-patient-safety-inititiatives-marion.

54 Imprivata, "Community Hospital Anderson Uses Imprivata Biometric Solution to Combat Patient Misidentification Crisis," news release, Aug. 2, 2017, https://www.imprivata.com/company/press/community-hospital-anderson-uses-imprivata-biometric-solution-combat-patient.

55 R. Berger, "CoxHealth Enhances Patient Safety and Security With New Biometric Technology," news release, Aug. 9, 2018, https://www.coxhealth.com/newsroom/coxhealth-enhances-patient-safety-and-security-new-biometric-technology/.

56 Imprivata, "St. Joseph Health System Is Making Checking In More Secure & Accurate With Biometric Identification," accessed May 9, 2022, https://www.imprivata.com/resources/video/st-joseph-health-system-making-checking-more-secure-accurate-biometric.

57 Imprivata, "Delivering High Tech, Patient-Centered Care With Secure One-Touch Desktop Roaming," accessed May 9, 2022, https://www.imprivata.com/sites/imprivata/files/2022-02/os-css-memorial-0318.pdf.

58 RightPatient, "Case Study—Terrebonne General Medical Center" (April 21, 2016), https://www.rightpatient.com/wp-content/uploads/2016/04/TGMC-case-study.pdf.

59 RightPatient, "University Health Care System Implements RightPatient® Biometric Patient Identification System With Epic EHR," news release, Aug. 16, 2016, https://www.rightpatient.com/university-health-care-system-implements-rightpatient-biometric-patient-id-with-epic-ehr/.

60 RightPatient, "Case Study—Iris Biometrics for Patient Identification" (2015), https://www.rightpatient.com/wp-content/uploads/2015/02/Novant-Case-Study.pdf.

61 M2SYS Healthcare Solutions, "Archbold Memorial Hospital Implements RightPatient Patient Safety and Data Integrity System," news release, July 1, 2014, https://www.m2sys.com/archbold-memorial-hospital-implements-rightpatient-patient-safety-system/.

pewtrusts.org