Health Care Can Learn From Global Use of Biometrics

Examples from other industries could offer lessons for linking patient medical records

Contents

The Pew Charitable Trusts

Michael Caudell-Feagan, *executive vice president and chief program officer*
Michael D. Thompson, *senior vice president, government performance*
Kathy Talkington, *director, health programs*
Ben Moscovitch, *project director*
Molly Murray, *officer*

Acknowledgments

Pew's health information technology project wishes to thank the following for their comments on the draft report: Lisa Bari, Blake Hall, Erin Mackay, Aaron Miri, Ellen Moskowitz, and Catherine Schulten. Although they have reviewed the report, neither they nor their organizations necessarily endorse its findings or conclusions. In addition, Pew thanks Daniel Bachenheimer, Elizabeth Naik, A.B. Patel, Suneeta Kudaravalli, Katarzyna Byszek, Meghan Yurchisin, Alexa Jaeger, and Emily Mitchell from Accenture for conducting the research underlying this report. We also thank current and former Pew colleagues: Josh Rising, Rita Torkzadeh, Bernard Ohanian, Zach Bernstein, Ken Willis, Matt Mulkey, Lindsay Henry, Shamyra Edmonds, Kimberly Burge, Tricia Olszewski, Ned Drummond, and Adrienne Tong for their valuable editing, guidance, and production assistance. Finally, we thank Rebecca Rachmany for freelance writing assistance.

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

Overview

Americans use scans of their fingerprints, faces, or eyes to access mobile devices, board airplanes, obtain admission into theme parks, and in numerous other ways to make everyday tasks more efficient. Across the world, individuals use these types of biometrics to obtain government services, bank, and travel.

Yet despite widespread use of biometrics in a range of industries, these tools are not employed in the United States to address a key problem that has plagued the health care system for decades: patient matching, or the ability to accurately link health records for the same person across different sites of care, such as multiple hospitals and clinics.

Patients often visit multiple health care providers, and patient records from one facility may have information on diagnoses, lab test results, or other data critical to providers at another institution. Accurate patient matching would help ensure that the doctors, nurses, and other clinicians caring for a patient across a range of health care facilities have the information they need to offer high-quality, coordinated, and safe care.

Current patient matching approaches in the U.S. typically rely on simple demographic data such as names, addresses, and/or birthdates. However, match rates when sharing this information among health care facilities can be as low as 50%, with errors resulting from typos, changing data (e.g., when patients move), similar data (e.g., same name and birthdate), and many other factors. Given the limitations of this demographics-based system, the federal government and Congress have examined alternatives, including whether to establish a unique patient identification solution, which could involve biometrics, assigning patients a number, or other solutions.

But the use of biometrics for patient matching across health care facilities presents several challenges. Sites may use different types of biometric (some facial scans, some fingerprints), have various brands of scanners, or store the biometric data in a format incompatible with other systems. At the same time, the sharing of interoperable—or easily exchanged—biometrics data may introduce privacy concerns. Further, different types of biometrics may not function as effectively with certain patient populations—for example, facial recognition may not be as effective in identifying people of color—and could increase existing health disparities. Finally, broad adoption of biometrics in hospitals and clinics across the United States would require the installation of technology, with corresponding cost and workflow changes.

To address these questions for health care in the United States, The Pew Charitable Trusts worked with Accenture, an international professional services company, to examine the application of biometrics worldwide and in other industries. Through a literature review and interviews, Pew and Accenture selected examples covering immigration, financial services, and other applications to assess the approach used and identify lessons learned for potential use in patient matching.

The examination led to several key findings:

1. **Barriers to and concerns about implementing biometric solutions remain.** Biometrics, as used today, are not a panacea for patient matching. Although current biometrics have some considerable advantages over other approaches, challenges remain with certain populations, including people of color because of technological inaccuracies, and the software used to match records remains imperfect.
2. **Recent innovations will make deployment easier.** Technological innovation may make deployment of biometrics nationwide more feasible in the coming years through the use of smartphones, tablets, commercial off-the-shelf (COTS) cameras, and even scanners built into credit card-size devices.
3. **Site- and person-centric approaches are emerging.** In some cases, use of biometrics in health care settings

would require technology implemented in a facility. In other cases, though, people can use their personal devices—such as smartphones—to scan and control their own information.

4. **Raw images are used for interoperability.** When different systems exchange biometric data, they typically share the raw images, such as a photo of a fingerprint, rather than proprietary templates, which are numeric representations of the biometric, to facilitate interoperability.
5. **Standards are necessary.** Biometrics, like other data, require use of standards for exchange among systems.
6. **Perceived benefits in convenience outweigh privacy issues.** Despite security and privacy concerns in the use of biometrics, its adoption and implementation continue to expand—in part because of the perceived convenience and accuracy in identifying individuals.
7. **Opportunities exist for mitigating privacy concerns.** Several approaches exist to protect sensitive data. Controlled access, audits, encryption, and risk mitigation strategies can help address privacy concerns, as could reforms to relevant laws.
8. **Government involvement can encourage adoption and adherence to standards.** As has been the case with the implementation of electronic health records (EHRs), government incentives and guidance can help drive adoption of biometric technologies. Further, setting technical standards to allow for interoperability can help ensure the exchange of data between entities.

In many ways, people have become more accustomed to the use of biometrics in their daily lives. But although biometrics have promise to improve patient matching in U.S. health care, a nationwide solution that supports interoperability, maintains privacy, and ensures equity remains out of reach without the resolution of key questions.

Once those questions are resolved and any lessons learned are applied, biometrics can enable better matching of records so that patients and their clinicians can have a more complete, accurate picture to inform medical decisions.

The fundamentals of biometrics

Biometrics refers to the measurement of physical or behavioral characteristics—such as the distance between ridges in fingerprints or voice cadence—that can help identify individuals. Biometrics can include fingerprints, facial imaging, and iris scans, among other forms.

Governments and police first employed biometrics in the late 19th century,[1] using fingerprints as a means of classification in order to exclude or reduce criminal suspects using the "Henry System." This was the first system to apply an index method to categorizing the physical characteristics of fingerprints.[2] The Henry System could not identify an individual, but rather cataloged the characteristics of the fingerprints so that authorities could exclude potential suspects who lacked those features. In this early implementation, investigators manually reviewed the fingerprints. By the 1960s, the practice of collecting and indexing fingerprints grew exponentially, and the FBI included them in more than 15 million criminal case files. Due to volume—and the rise in the use and functionality of computers—the need for an automated system to electronically match fingerprints became both pronounced and possible.

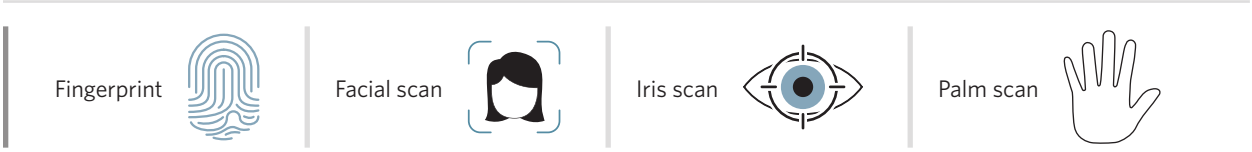
The FBI contracted with the National Institute of Standards and Technology (NIST) to determine how to develop an automated system for fingerprints in 1967. NIST found three key requirements for such a system: 1) scanning the fingerprint; 2) identifying the minutiae, or the specific characteristics, that would enhance indexing; and 3) an algorithm for the process of comparison.[3]

This technology has advanced, and matching algorithms can now assess a range of modalities—or the specific physical trait used for identification, such as iris scans or facial images. Although fingerprints and facial imaging remain the most commonly used modalities globally, some applications use iris or palm vein scans.[4] Additional types of biometrics, such as voice identification and gait recognition, are also in development stages and early applications.[5]

Along with an expansion of modalities over the decades, the use cases grew beyond criminal investigations. Many industries around the globe implemented biometrics to identify individuals and allow them to receive public services, cross international borders, board airlines, pay for goods, and perform other routine tasks.

To design biometrics for use in patient matching, the U.S. health care industry should consider three key foundational elements: the modalities, the format of the data, and the structure of the database.

Modalities for consideration



Many of the known biometric uses utilize fingerprints or facial images as the chosen modalities; several use both. Immigration, border control, and criminal investigations often choose fingerprints as a method of identification because of their consistency over time and unique characteristics, as well as for ease of collection.[6] Officials often collect fingerprints with an optical sensor that takes a digital image of the finger's surface and displays the patterns—whorls, loops, arches—as well as the location and directions of these characteristics. These details provide the information needed to better confirm individuals' identity through matching.[7] NIST adopted standards for fingerprint minutiae and images that dictate image quality and format; it also developed standards for exchanging these images.[8] There are also several international standards that define biometric exchange and quality that are used by public and private institutions globally and in conjunction with standards identified by NIST.

Despite the widespread use of fingerprints, certain medical conditions inhibit collection. Individuals with skin or genetic conditions such as leprosy or eczema can lose the ridge patterns that are used in matching algorithms.[9] For these individuals, fingerprints cannot reliably verify their identity.

Instead, many civil agencies, as well as private sector industries such as travel or online banking, implement facial recognition systems. Humans use faces to recognize and identify each other; the algorithms that process and match facial images today do so with either a feature- or view-based approach.[10] Feature-based algorithms assess facial characteristics such as eye placement and nose shape, while view approaches normalize the face and account for lighting and expression differences.[11] NIST adopted standards for format and quality of facial images and, given advances in smartphones and digital cameras, many COTS products meet these guidelines.[12]

Although faces, for the vast majority of individuals, are typically public as they can be seen when individuals leave their home, concerns about the government collecting images without consent have surfaced.[13] Cameras can capture a clear facial image from a distance, without the individual's knowledge or consent.[14] Additionally, research has shown that the algorithms used in facial recognition are less accurate for people of color, specifically for Black women.[15] The particular role and use of facial recognition by law enforcement has also come into question; notably, that law enforcement agencies can use the software without individual consent, for a variety of purposes, including mass surveillance.[16]

However, there are differences in accuracy when using facial recognition for a one-to-one match—for example, a selfie to a passport image—compared to a one-to-many match, such as comparing a passport image to photos of all passengers in a flight manifest.[17] The one-to-one match is often more accurate, comparatively, than comparing a single photo to multiple images.[18]

A scan of the iris can also be used to confirm identities because of its unique and structurally distinct patterns. The use of iris images can easily discern between individuals—even identical twins—and the collection of the biometric, when it meets international standards, is not affected by contacts or other corrective lenses.[19] Unlike a retinal scan that uses blood vessel patterns, iris recognition relies on the iris muscle.[20] The international standards for capturing an iris image ensure the scan is of high-enough quality to provide accurate matches. However, scanners can use infrared radiation to collect the iris image, which has the potential to cause damage to the iris.[21]

Other hand-based modalities, such as palm print recognition, use similar models to fingerprints, as palms also have unique characteristics such as ridges. However, the sensors that collect the palm image must be large enough to scan an individual's hand. Hand-based modalities can also present challenges in collection and accuracy of scans for individuals with arthritis and similar conditions.[22] Many other biometric modalities exist, including behavioral markers such as gait, voice, or signature, but they are not as broadly used in consumer-facing applications compared to facial recognition, fingerprint, or iris.[23] Each behavioral marker has specific implementation considerations.

Formats differ from image to templates

For all modalities, organizations store the biometric as raw images or templates, and sometimes both. The raw image represents the initial digital representation of the modality, such as a photo that a human could interpret without computer assistance. However, matching algorithms cannot process raw images and require the use of templates, which represent the image in a numerical form. These templates are often proprietary—meaning specific to a certain system or vendor. Patient matching algorithms are unable to compare different proprietary templates, thus inhibiting interoperability.

The exchange of raw images supports interoperability as different systems could use the image to create their own proprietary templates for comparison. However, sharing of raw images holds a higher risk if breached, as hackers would then have information on individuals that can't be changed. On the other hand, hackers typically cannot reverse-engineer templates back to the original image, thus protecting privacy. Yet proprietary templates don't support interoperability across systems.

Neither templates nor images can be matched across modalities: For example, algorithms can compare templates of different fingerprints, but cannot compare fingerprints against a facial image. Matching works only within a single modality.

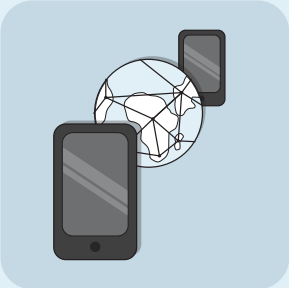
Key Biometric Standards

The National Institute of Standards and Technology (NIST) was established by Congress to keep the U.S. at the cutting edge of science. Today, NIST develops technology, measures, and standards in order to advance science and spur innovation. It determines many of the technical standards used in biometrics.[24]

The International Organization for Standardization (ISO) develops and publishes global standards for a wide range of industries so that technology can work across borders. This includes creating and advancing many technical standards used in biometrics.[25]

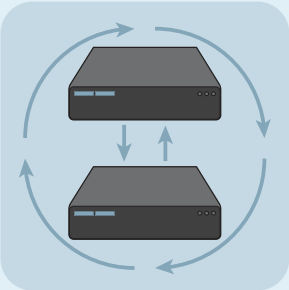
Storage approach affects architecture decisions

Databases store biometric images and/or templates. There are three possible database configurations:



Decentralized: Dispersed databases store biometric data locally—on a trusted smartphone or hand-held device. For matching to work in a decentralized model, users either enroll on a personal device or biometric data is downloaded to it. NIST defines a decentralized network as: "A network configuration where there are multiple authorities that serve as a centralized hub for a subsection of participants. Since some participants are behind a centralized hub, the loss of that hub will prevent those participants from communicating."[26]

Centralized: A single, centralized system is used to enroll and search all biometric data. NIST defines a centralized network as: "A network configuration where participants must communicate with a central authority to communicate with one another. Since all participants must go through a single centralized source, the loss of that source would prevent all participants from communicating."[27]



Federated: A single source sends data to multiple systems, all of which are then used to enroll and search biometric data. The user must search all systems and aggregate the responses. NIST defines federation as: "A process that allows the conveyance of identity and authentication information across a set of networked systems."[28]

Patient matching and biometrics intersect

Patients often receive care from different providers at a variety of facilities—sometimes across states—leading to individuals with multiple, incomplete health records in separate EHR systems. Clinicians often require information from other records to make appropriate treatment decisions informed by a complete history and up-to-date health information. Yet this exchange and subsequent patient matching fails up to half of the time.[29] The challenges in matching can lead to patient safety issues; for example, merging records incorrectly could result in unneeded and potentially dangerous treatment, while not matching a patient's disparate records might mean providers are unaware of pertinent allergies or medications.

Patient matching generally occurs through a combination of approaches, including use of algorithms and manual review, and relies on demographic data such as names, dates of birth, Social Security numbers, and addresses. Different systems and technologies—such as EHRs and health information exchange (HIE) systems—navigate patient matching issues using varying approaches, including by integrating external information.[30] However, human error—such as typos, changes in demographic attributes because of life events, and nonstandard data across systems—inhibits matching and contributes to low match rates.[31]

Lack of standardization and uniqueness contributes to patient matching challenges

Congress recognized this patient matching challenge more than two decades ago. Although Congress in the Health Insurance Portability and Accountability Act (HIPAA) in 1996 required the establishment of a national patient identifier, lawmakers have banned the use of federal funds toward that end since 1998.[32] The House of Representatives approved an amendment to strike that ban in 2019, but the restriction remains law today.[33] Instead, in 2020 Congress charged the Office of the National Coordinator for Health Information Technology (ONC) with assessing current and potential approaches to improve patient matching and to produce a report covering potential solutions.[34]

In 2009 Congress, through the Health Information Technology for Economic and Clinical Health Act, provided incentives for the use of EHRs. Although this resulted in an increase in their use, it did not require data standards for demographics or exchange.[35] The lack of standardization in the documentation of data elements and the inability to uniquely identify individuals in EHRs contribute to errors in patient matching. The initial certification criteria that the ONC sets for health record system functionality did not include standards or requirements for the inclusion or documentation of demographic data elements. Although more recent regulations require certain standard data elements for exchange—including demographic information—these changes, while important, will not completely resolve matching challenges. Health care should continue to investigate additional solutions for improving match rates beyond the use of demographic data standards.

Biometrics offer promise

Given the ongoing difficulties with patient matching and identifying individuals, health care has increasingly considered a solution regularly used in other industries: biometrics. People use biometrics every day—to access smartphone apps, unlock a car, or authorize payment for goods or services. In fact, in 2017 Pew conducted focus groups where patients overwhelmingly supported the use of biometrics for identification and matching, as opposed to the use of smartphones, remembering to carry a card, and other options.[36] Unlike a number or a card that a patient must memorize or bring with them to an appointment, people always "carry" their biometric identifiers.

Yet, biometrics have not been adopted in the health care industry. When health care organizations do implement biometrics, they use them for patient identification within a single system to locate individuals' records. Conversely, facilities that use biometrics typically don't employ them to match records across different organizations.

Biometrics could aid patients because of their persistency, meaning that people will generally have them, and convenience—they cannot be forgotten at home like a card. However, what makes biometrics appealing can also present problems: Biometrics never change. If a security breach occurs that compromises an individual's biometrics, the patient's identity remains at risk for fraud as physical features do not change. Solutions that promote interoperability across systems further heighten these security concerns given the dissemination of biometrics into more databases.

However, other industries—such as travel and security—have found ways to design and implement biometric solutions that allow for flexibility, privacy, and interoperability across different organizations. Although no example represents a direct or complete analog to health care in the United States, these models can provide lessons learned on how to design a biometrics solution for cross-organization patient matching.

Key factors inform biometric use and applicability to health care

Health care should assess several considerations that may not appear in other industries before broadly implementing a biometric model for cross-organization matching. These factors include: privacy, equity and discrimination, and access.

Privacy and security considerations: The sensitivity of health and biometric data—and the associated breach concerns—highlights the importance of securing and limiting access to biometric data. The federal government oversees privacy of some health data today, such as through regulations implementing HIPAA and additional protections for behavioral health data (referred to as 42 CFR Part II). Many of these same privacy protections could—and already often do—apply to biometric data. However, these policies also permit the use of data in certain ways, such as for improving operations and even research in some cases.

Equity concerns: Health care should also consider issues around equity when determining the scope and practice of biometrics. As research has shown, some patients already experience inequities in health care because of a variety of socioeconomic and structural factors, including systemic racism and religious discrimination, and a technological solution for matching should reduce, not increase, these inequities.[37] For example, as mentioned, facial recognition technology does not function as effectively for people of color and could therefore fail to avert patient matching-related medical errors that would be addressed for White patients. The use of this approach, if unaddressed, could result in communities of color not benefiting from improved matching. At the same time, use of biometrics may also provide opportunities to match records that otherwise wouldn't be linked—such as for homeless populations who may not provide consistent contact information.

Access to biometric solutions: For biometrics to improve patient matching, all facilities and patients across the country need equitable access to the required technology and hardware—which means addressing concerns around cost, broadband access, and network connectivity. Implementing biometric solutions not only carries an initial cost but also requires maintenance, hardware upgrades, and software updates. These costs could remain out of reach for smaller health care organizations and stand-alone physician practices.[38] Further, limited access to broadband could make rural communities unable to implement the same software as other parts of the country, and network connectivity issues in densely populated urban areas could cause problems with processing speed.[39]

Approach to identify biometrics examples

Given the many complexities associated with the use of biometrics, Pew sought to understand the experience in other industries and internationally in using different modalities to link records. Pew worked with Accenture to develop 10 examples that identify lessons learned for health care in the United States.

Pew and Accenture sought a diverse set of examples and selected them based on five criteria:

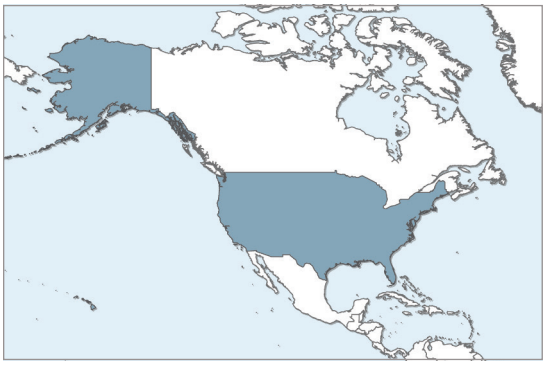
- *Cross-entity:* Whether the example involves the exchange of biometrics between databases, with a preference for the sharing of data between organizations
- *Geography:* Where the example occurs, with a priority for diverse implementation sites
- *Industry:* Which industries use biometrics, with an attempt to draw on a range of applications
- *Timing:* When the biometrics were used, with a focus on more recent applications
- *Modality:* Which modalities were in use, with an emphasis on diversity to illuminate differences across modalities

Prior to selecting 10 examples, Pew and Accenture identified 28 potential cases of biometrics use (see Appendix I). Pew and Accenture then culled that list to 10 examples that would highlight a diverse set of lessons learned that are most applicable to health care in the United States, with a focus on workflows, technical considerations, privacy implications, and implementation. The selected examples purposely span different types of industries to demonstrate the wide use of biometrics and provide insight for health care on designing a solution with the intent of improving patient matching. If multiple examples highlighted similar lessons learned or designs, only one of the models was chosen.

The examples, grouped by industry, start with more common uses and increase in complexity. The later examples use biometrics in ways that many Americans may not yet experience or envision, such as to receive social welfare benefits. The industries and associated uses are:

- **International travel**
    - Customs and Border Protection's Biometric Exit
    - World Economic Forum's Known Traveller Digital Identity
- **User-driven identity confirmation**
    - Mastercard's biometric authentication credit card
    - Provider authentication for electronic prescribing of controlled substances
- **Border security and immigration**
    - Department of Homeland Security's US-VISIT program
    - Five Country Conference Protocol
    - eu-LISA Visa Information System
- **Digital identity to access public services**
    - Estonia's national e-ID card
    - India's Aadhaar program
    - ID2020

Customs and Border Protection Biometric Exit program



Location	United States
Industry	Travel
Department/agency	U.S. Customs and Border Protection
Modality	Facial scan
Use	Paperless airline boarding
Storage	Centralized cloud-based database

U.S. Customs and Border Protection (CBP) implemented a pilot program in a limited number of airports that employs biometrics to streamline travel. It developed a system that uses facial recognition to preclude the need to present a passport while traveling. Participating commercial partners—such as airports, airlines, or cruise lines—let passengers opt in to the service, which captures images of travelers' faces at boarding. If the CBP system finds a match to the photos on file, travelers can board their flight or ship—and in some instances go through customs—without presenting their passport.

Six sea entry ports and 34 airports use this program, and three airline partners and one cruise line implemented the system for document-free boarding. The service uses passenger manifest data, which includes travelers' demographic information and existing photographs (such as from passports), to confirm individuals' identity by comparing the images against those captured during boarding. The commercial partner will receive a message from the system that a match was found, and the traveler is not required to show a passport or a ticket to board a flight or go through customs.

Workflow

When individuals book their travel, they supply basic demographic information to the commercial airline or other carrier. This information creates the manifest that contains all expected passengers and their basic demographics (name, birthdate, gender, and address), which is sent to CBP. This information is used to create a gallery of the passengers, pulling from existing demographic information and photos already on file (obtained from prior CBP encounters, or from other federal agencies, such as the U.S. Department of State). The CBP system converts the raw images to templates then performs identity verification throughout the travel process.

When the passenger queues to board the flight, CBP officers or airline personnel capture a photo of the individual at the gate (where a boarding pass and passport would usually be scanned) using commercially available technology, such as a tablet or webcam. The camera system used at the gate sends the image to the CBP system, which converts the photo to a template and compares it to the images in the photo gallery using a matching algorithm. The airline receives a yes or no response within seconds that indicates if the passenger matches the flight manifest and can board without using a passport. If a match isn't found, the passenger uses a physical passport and boarding pass.

Technological and other key characteristics

Airlines and cruise ships can use COTS cameras, including tablets and standard webcams, to capture images only if the device has a network connection. After initial testing of matching using images from COTS cameras, CBP had successful match rates in the high 90s.[40] The composition of the photo must meet the CBP-determined quality standards in order to be used by the matching algorithm, including the position of the head of the traveler, and the percentage of space the

head must fill within the photo. When taking the photos, CBP requires that the airlines or cruise lines:

- capture multiple images;
- ensure travelers look directly at the camera;
- include a "timeout" function in technology that sends the best image even if none meets the desired quality threshold; and
- provide proper lighting.

The CBP system is a secure cloud-based database with restricted access. For CBP staff who are granted access, two-factor authentication is required.[41] Air and cruise lines do not have access to the images, and they do not retain photos in their systems. Airline and cruise ship officials will see only a positive or negative match confirmation from the system.

Airports and other travel locations did not adjust their network infrastructure or bandwidth in preparation for using the CBP system. In some cases, this resulted in delays in system implementation and in capturing images, exchanging data, and matching results once it went live.[42]

Any U.S. citizen may opt out of the CBP Biometric Exit program and choose not to have their image captured.[43] If opting out, travelers will go through a manual process, including a CBP officer or airline official reviewing their passports and boarding documents as typically occurs absent this program.

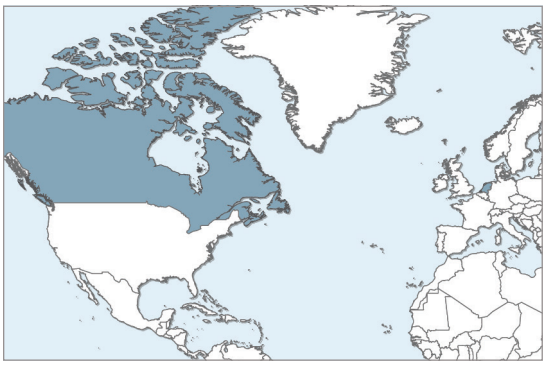
To ensure that privacy protections and matching algorithms remain current, CBP conducts routine testing and system audits. As the system continues to be used and with more travelers, there is more data available to assess match rates and ensure the highest possible confidence in match determinations.[44] This data is used to update the system and improve the match rates.

Lessons learned

The application of facial recognition by travelers underscores three lessons important to applying biometrics in the U.S. health care system: using commercially available technology, ensuring adequate infrastructure upgrades, and mitigating privacy concerns.

1. **Use of COTS equipment:** This example highlights how facial recognition, unlike some other biometric modalities, can succeed with COTS cameras and equipment, including tablets and other standard webcams that are widely available. The use of COTS can lower the cost of implementing facial recognition within health care without sacrificing quality.
2. **Infrastructure upgrades:** As demonstrated by bandwidth challenges at airports, biometric use can increase traffic on an organization's network and lead to delays. Implementation of biometrics for cross-organization matching may require hospitals and other facilities to adjust or upgrade that infrastructure and networks and monitor traffic for challenges that emerge.
3. **Mitigate privacy concerns:** CBP implemented several layers of security protections, including private network connections, dual-factor authentication, and limitations on user access. Similar approaches could mitigate concerns in health care. Encrypting information within databases and during exchange also adds to the privacy of the sensitive data.

World Economic Forum Known Traveller Digital Identity project



Location	Canada, the Netherlands (initial pilot)
Industry	Travel
Department/agency	World Economic Forum
Modality	Facial scan
Use	Passport-less international travel
Storage	Decentralized database

Similar to the CBP Biometric Exit program case example, the Known Traveller Digital Identity (KTDI) project has the ultimate goal of eliminating the need to present passports and boarding passes in international travel. The KTDI project works across stakeholders—government agencies, sectors, and countries—to allow travelers to use a smartphone application as their identification when traveling.

Although many travelers store boarding passes within airlines' smartphone applications, passengers can also use the KTDI app to store and manage their identity information (passport data, photo, and flight information). From the app, they can consent to share the identity information required by a particular entity, including facial photographs, with border authorities, airlines, and other partners in advance of their travel. At specific checkpoints and throughout their travel, biometrics are used to confirm their identity.

As of April 2020, the KTDI project remains a pilot program and can be used in three airports globally: Montreal-Trudeau International Airport, Toronto Pearson International Airport, and Amsterdam Airport Schiphol. Air Canada and KLM Royal Dutch Airlines participate in the program and plan to use the KTDI app as a digital form of identity for up to 10,000 travelers throughout the pilot.[45] To join in the pilot, the traveler must be invited to create a digital wallet that contains the identity information using the KTDI app through participating airlines.

Workflow

To participate in the program, the traveler first creates a username and password via the KTDI app and can elect to use the mobile device's biometric verification in place of a password (e.g., fingerprint or facial recognition, depending on the device). Once in the app, the traveler creates a profile.

After the digital profile is set up, the traveler goes to a local government office to verify their identity. To do this, they supply their passport to a government official and have a digital picture taken. Both pictures—the new one and the existing photo image, which is accessed through the chip on the physical passport—are converted into templates and run through a matching algorithm; this step ensures that the passport belongs to the traveler. Upon match confirmation, the recently taken photo is deleted.

Once the match is confirmed, a QR code is created and displayed on the government official's computer. The traveler opens their KTDI app and scans the QR code, which creates a secure connection between the government computer and the mobile device, allowing for data exchange between them. Through the secure connection, the government official sends a mobile passport to the KTDI app, which includes demographics and the digital facial photo image that were pulled from the passport via its chip. The facial image, along

with demographic information, is stored on the user's mobile device in the KTDI app. The traveler now has a government-approved mobile passport in the KTDI app. Before their travel begins, the traveler can elect to share their mobile passport with the airline and border control.

When using the KTDI app prior to travel, the raw images are encrypted and sent to the stakeholder's biometric system, where they are converted into templates. There is a KTDI lane at security, boarding, and border control, where live photos are taken of passengers. The images of those photos are also sent to the biometric system, where they are converted into templates, and facial recognition is used to compare the live image with the photo from the mobile passport. If a match is found, the traveler can proceed without needing to use a passport or boarding pass.

Technological and other key characteristics

KTDI uses a decentralized identity model, meaning that there is no central authority needed to validate an identity claim, with the user controlling the access. Travelers maintain the data on their smartphones for the duration of the KTDI pilot, and the stakeholder's biometric system containing the image galleries used to confirm identity is frequently purged, often 24 hours after travel is completed.

The photo must be a passport photo that is compliant with the International Civil Aviation Organization standard, which is based on the International Organization for Standardization (ISO) standard.[46] These standards control for quality, format, and size, among other image requirements.

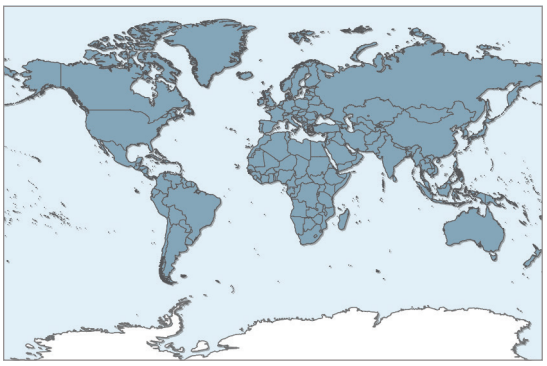
When users elect to share data from the KTDI app, they can see when and by whom their data is accessed and viewed.

Lessons learned

The KTDI example demonstrates two key lessons on the power that individuals can exercise over their digital identities:

1. **The use of standards:** KTDI works across industries and among public sector agencies because these stakeholders agree upon and commit to the use of standards, as they did with ISO facial image standards. As health care implements and uses many standards—including code sets to document diagnoses, order labs, and send claims—the industry is capable of adopting them, when the benefits are clear.
2. **User control as a privacy lever:** In the KTDI process, individuals not only control who can access their digital identities but can also see an audit trail. Putting people in charge of their data can help with uptake in participation in programs that use biometrics, and audit trails can act as an important mechanism for transparency. In health care, allowing patients to be in control of their biometrics and increasing transparency around how their data is used could help with adoption of this technology.

MasterCard's biometric payment card



Location	Global
Industry	Finance
Department/Agency	Private sector
Modality	Fingerprint
Use	Payment
Storage	Digital chip on payment card

Mastercard created the first payment card that uses biometrics to verify individuals' identity for purchases in lieu of a personal ID number (PIN) or signature. The technology inside the chip on the card allows users to scan a fingerprint by placing it on the card's embedded sensor to authenticate who they are during a purchase. Merchants do not need to purchase additional hardware, as the biometric reader is the card itself, powered by the standard EMV (Europay, Mastercard, and Visa) terminal in use worldwide.

This biometric card uses existing merchant hardware and transaction messaging as part of its solution. It functions as an alternative method of authentication confirming that the person is permitted to make the purchase without the need for a PIN or signature. The user experiences a checkout process that is as fast as current contactless transactions, while keeping sensitive biometric data on the card itself. Additionally, the results of the biometric match are shared with the issuer as part of the authorization request.

Workflow

Cardholders can enroll for the biometric card at home using battery-powered "self-enrollment devices," which are available from card vendors. In a typical use case, the cardholder inserts the biometric card into the device, providing power to the card for enrollment. After the cardholder completes the enrollment, they then contact the card issuer to activate the account and verify their identity.

If the card will be used for the distribution of formalized benefits, such as disbursements or insurance benefits, enrollment is an in-person process. The cardholder provides demographic information and a government ID to confirm their identity. The cardholder is either given the enrollment device as above or uses a tablet to capture fingerprint images. The fingerprint images are converted to a template and transferred for storage onto the card.[47] The card is then activated. In either case, the biometric data is stored securely as a digital template on the card and never shared externally.

Once the templates are stored on the card, the cardholder can begin to use it normally. The cardholder inserts or taps the card at a terminal at purchase, placing a thumb on the card's sensor. The thumbprint is compared against the stored biometric template on the card. If it was successful, the cardholder does not need to complete any additional steps. If the match fails—after a set number of attempts that merchants can determine for themselves—the card automatically switches to the next cardholder verification method enabled on the card using either a PIN or signature so the transaction can still be completed.

Technological and other key characteristics

The biometric card complies with the same standards as a regular payment card and can be used in any EMV terminal. For most effective workflows, the terminal should be:

1. customer-facing;
2. accessible to cardholders; and
3. designed so the card sensor is not blocked from use for contact transactions.

For contactless transactions, the card can be used by tapping or hovering it close to the contactless indicator on the terminal.

The template of the cardholder's fingerprint is never shared with the merchant.[48]

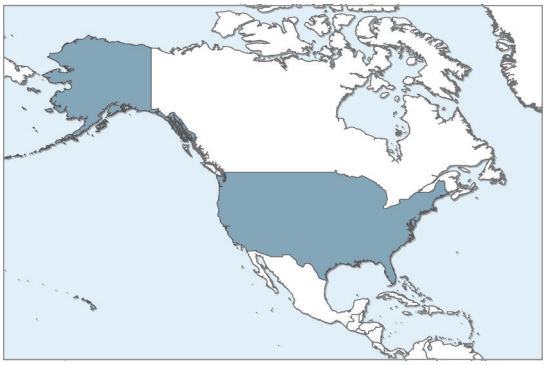
If the card is lost or stolen, individuals use the typical procedures for canceling and replacing a card. The card issuer would deactivate the account, and the card would not be usable.

Lessons learned

This case study demonstrates the increased accessibility and acceptance of biometrics in everyday activities, as well as that biometrics provide an accessible approach for identity verification:

1. **Accessible authentication options:** Biometric cards can be a simple tool for identity authentication and verification. A biometric card could become a health insurance card, acting both as insurance and identity confirmation, and is already something patients are accustomed to bringing to medical appointments.
2. **Multiple solutions for authentication:** Biometric cards have backup authentication methods, such as using a PIN. If the matching fails, there is a safeguard for individuals in real time.

Provider authentication for electronic prescribing of controlled substances



Location	United States
Industry	Health care
Department/agency	Private sector
Modality	Facial scan
Use	Two-factor authentication
Storage	Centralized database

A new federal law aimed at combating the opioid crisis requires physicians to start electronically prescribing—sending a digital prescription to a pharmacy, rather than a paper slip—controlled substances in a manner compliant with the Drug Enforcement Administration's (DEA) rules and standards for digital credentials by Jan. 1, 2021.[49] The DEA requires two-factor authentication, or providing two sources to confirm identity, for a provider to electronically prescribe controlled substances (EPCS). Allscripts, an EHR developer, and ID.me, a biometrics company, designed a solution to streamline electronic prescribing for controlled substances such as opioids.

Normally, EPCS requires multiple steps and the use of an external device, such as a fob, that generates a custom code. Through this approach, providers can use a smartphone application that transmits identifying information for two-factor authentication to meet the DEA requirements.

Workflow

First, the provider downloads the ID.me app and enters their EHR user information, such as a username and password. The clinician then receives an email to their EHR and app accounts. After clicking the link to make the connection, the provider sets up multifactor authentication by entering a security code received via text into the app.

The provider then uploads both a photo of a government-issued identification—a passport or driver's license—and a selfie taken in real time into the app. ID.me compares the image from the government ID with the photo using facial recognition.[50] Both of the images are stored in the ID.me database as encrypted raw images.

After the above steps, the provider can use ID.me to provide two-factor authentication for EPCS. Using the standard electronic prescribing workflow within Allscripts, the physician can place the order for the controlled substance. The provider will then open the ID.me app and see an automatically generated six-digit code to enter within a field in the order as the second factor needed for authentication. The clinician can then sign and send the electronic prescription to the patient's preferred pharmacy.

Technological and other key characteristics

Armed security guards, surveillance equipment, and access control technology secure the servers hosting biometric images.[51] This approach helps protect the data from both physical and cyber intrusions.

The biometric selfies follow NIST Identity Assurance Level (IAL) 2 standards for quality, which include

requirements on image resolution, pixels, and color and is the standard used for government-related transactions (NIST defines IAL2 as follows: "Evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity. IAL2 introduces the need for either remote or physically-present identity proofing."). [52] Photos can be captured on any mobile device with a functioning camera and network connection. [53]

For the photos used at registration, liveliness (meaning the image was taken live and not uploaded from a stored photo) and anti-spoofing detection, used to ensure the image is coming from the appropriate source, prevent the use of photographs of other individuals. [54] These processes follow a NIST framework that stipulates how to complete the identity-proofing process with minimal security risk. [55]

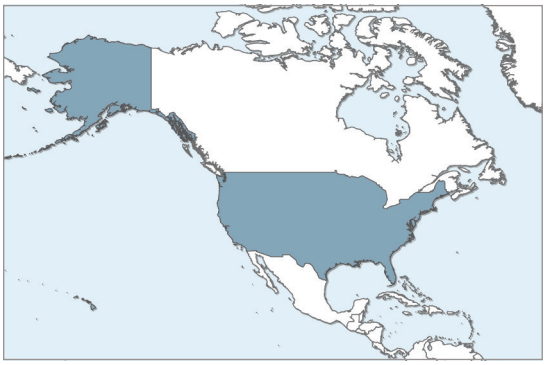
The ID.me process of verification and the associated creation of a digital identity follow the principles developed by the National Strategy for Trusted Identities in Cyberspace (NSTIC). Launched in 2011, NSTIC is a government initiative that encourages collaboration across private and public sectors to improve the efficiency, safety, and security of online interactions, including digital identities. [56] The principles state that credentials should be: privacy-enhancing and voluntary, secure and resilient, interoperable, and cost-effective and easy to use. [57]

Lessons learned

This example highlights the security measures for central databases and the role that individuals' smartphones can play in collecting biometrics and confirming identity:

1. **Centralized databases can be secure:** Although many concerns over the use of centralized databases focus on breaches, there are ways to provide multiple layers of security to protect sensitive data. ID.me stores raw images and has designed access controls, auditing, and physical security to protect this information. If health care organizations use central databases, multiple layers of protection for sensitive health information could reduce the likelihood of unauthorized data access. There is, however, an associated cost that comes with physical security and extensive auditing and access control.
2. **Role of smartphones:** As demonstrated by this example, smartphones typically available for consumers can take the photos as well as transmit the needed information, perform facial recognition, and share back a response on match status. As most patients have smartphones, this system provides a feasible and low-cost way to capture a biometric and can act as a form of identification from wherever patients and their smartphones are located.
3. **Users have sole control:** Following the NSTIC principles, in this example users have control over their data—in this case, the choice of whether to use this approach for two-factor identification or revert to other approaches. Individuals opt in to the process, can choose to delete their digital identity at any time, provide consent for sharing each data element, can view what data elements have been shared and with whom, and can revoke access at any point. Giving the user this level of control empowers individuals to determine what to share, with whom, and for what purposes. As patients become more empowered through access to personal health information, this level of control over biometric data could help address concerns about privacy, security, and inappropriate usage.

Department of Homeland Security US-VISIT program and the IDENT database



Location	United States
Industry	Immigration/travel
Department/agency	Department of Homeland Security
Modality	Fingerprint; limited facial scan and iris
Use	Immigration and border control
Storage	Centralized database

The Department of Homeland Security (DHS) implemented a program that uses biometrics for security purposes at border control and points of entry into the U.S. The U.S. Visitor and Immigration Status Indicator Technology, or US-VISIT, program uses fingerprints and facial scans to identify all non-U.S. citizens who enter and exit the country. US-VISIT maintains a centralized database, referred to as the Automated Biometric Identification System (IDENT), to reduce the use of fraudulent travel documents and ensure that individuals entering the country are not known or suspected terrorists, criminals, or immigration violators.[58] Federal agencies use IDENT to ensure that individuals entering or exiting the country are who they claim to be—and that their identity matches the demographic information on their travel documents and applications.

IDENT was the original database for fingerprints collected by border control in the 1990s.[59] The US-VISIT program expanded IDENT to collect fingerprints and facial scans in international airports and additional ports to grow the database and confirm identity of non-U.S. citizens when they entered the country.

Several other federal agencies—including Citizenship and Immigration Services (CIS) and the Department of State—send raw images to IDENT as well. These images come from visa applications, past visits to the U.S., or criminal records.

US-VISIT is in place in 115 airports, 15 seaports, 101 land border stations, and 211 visa offices worldwide.[60] It contains more than 200 million fingerprint records, 36.5 million facial scans, and 2.8 million iris scans.[61]

US-VISIT and the widespread collection of biometrics, particularly facial scans, were subject to scrutiny by the House Committee on Homeland Security in 2019.[62] The committee raised concerns regarding security of the data because of a CBP system breach early in 2019, as well as issues with facial recognition software misidentifying people of color.

Workflow

The US-VISIT program collects biometrics of non-U.S. citizens and stores the raw images within IDENT. The process begins either in a traveler's home country at a U.S. visa-issuing post, such as a consular office, if the traveler is required to travel with a visa or upon arrival in the United States if the traveler is from a visa-waiver country. In the case of the former, the traveler goes to the closest U.S. visa-issuing post and meets with a Department of State consular official. There, a U.S. government representative interviews the traveler and collects biometrics: 10 digital fingerprints and a digital photograph. The raw images of those biometrics become part of the IDENT database.

Once travelers arrive in the United States, a CBP official reviews travel documents, scans 10 fingerprints, and takes a digital photo. These images also become part of the person's record in IDENT and are assessed for a match to the existing images in the database. To determine a match, the images are sent to the IDENT biometric vendor, where they are converted into proprietary templates and assessed for a match against the templates of biometrics already on file. Upon finding a match, the CBP official obtains information on past travel, visa status, and whether the individual is on a criminal or terrorist watch list. Based on the information received, the CBP official processes the traveler's entry accordingly, such as by allowing entry or detaining for further questioning.

If biometrics for this individual are not in the database and no match is found, the CBP official relies on travel documents and interviewing the individual before determining whether to permit entry into the country.

There is no permanent biometrics process at departure; the biometric exit process described here is currently being piloted. Instead, airline manifests complete the exit process. In the future, DHS plans to implement a similar biometrics process at exit as well.[63]

Technological and other key characteristics

IDENT uses international standards (American National Standard for Information Systems/National Institute of Standards and Technology—International, or ANSI/NIST-ITL) for raw image and data quality as well as for data exchange to enhance interoperability. These include specifications for image resolution, the percentage of the image that should be filled by the subject's face, and overall dimensions.[64]

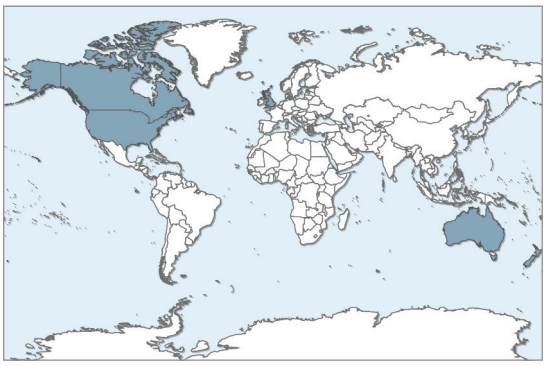
IDENT is a centralized database, and user access is restricted and monitored.[65] Because so many U.S. government agencies provide and query the data, DHS controls access and limits the availability of information. If a user requests information and does not meet the security requirements to view data, IDENT does not return results.[66]

Lessons learned

The US-VISIT process collects and stores raw images of multiple modalities for several purposes, revealing two lessons for health care:

1. **Raw images provide flexibility:** Although the storage of raw images elicits security concerns, the images enable matching when aggregated from a variety of organizations and systems with limited barriers. These images can also be collected and compared when captured by different technologies, such as digital cameras or smartphones. Unlike with the exchange of templates, health care organizations could share raw images between facilities and databases for matching purposes without running into issues with vendor-lock or proprietary templates.
2. **Multipurpose uses:** The images in IDENT are used for several different purposes: confirming identity, processing visa entries, identifying suspected terrorists, and reducing fraud, among others. By collecting and storing biometric images, health care could also find multiple purposes for them, with appropriate patient consent. Health care organizations could use images for patient matching but also identity verification when administering medications in the hospital or dispensing prescriptions to patients.

Five Country Conference Protocol



Location	United States, Canada, United Kingdom, New Zealand, Australia
Industry	Public safety and immigration
Department/agency	U.S. Department of Homeland Security
Modality	Fingerprint
Use	Immigration and security
Storage	Federated (centralized databases in each country that can be accessed by each participating country)

The Five Country Conference (FCC) Protocol is a collaboration among the United States, Canada, the United Kingdom, New Zealand, and Australia to share biometric data to enhance immigration and border operations and security. Each country allows the others to search their biometric database for matches when reviewing and processing immigration applications, including asylum and refugee determinations, using specific criteria. These criteria include: if the identity of the applicant is unknown or uncertain; if the applicant's current location is unknown; or if there is reason to believe that the applicant has spent time within one of the participating countries.[67]

Each country maintains a database containing biometric data of individuals who enter their country. All five countries include fingerprints; several also incorporate additional modalities. The U.S. database IDENT (discussed in the case study on the US-VISIT program) contains biometrics of non-U.S. citizens who enter and exit the country. The country's relevant agency queries the applicable country's database to search for a match for a specific applicant and receives information back.

The FCC Protocol began in 2009 and shares nearly 3,000 individuals' biometric data among the five participating countries each year.[68]

Workflow

Each country's immigration authority collects biometric data on individuals applying to visit the country, either through a visa or as a refugee seeking asylum. The collection of biometrics begins either at a consulate or visa-issuing office or at ports of entry, including airports, seaports, and land crossings. If travelers require a visa, they go to the closest visa-issuing post at their point of origin. There, a U.S. government official interviews the traveler, reviews the visa application, and collects the biometrics. These raw images become part of the participating country's biometric database. This is the same initial process used in the IDENT example.

If any of the partner countries identify an individual who meets the criteria, that country can query the system of the other nations for a match. The requesting country sends the raw biometric images it collected using a shared standard messaging format.[69] The providing country works to respond to the request within 72 hours with match information.

When one country queries another's database, a two-part process ensues. First, a message, containing only the raw fingerprint images, is sent through a firewall to a secure server hosted by the Australian government. That server works as the central processer for the requests and passes along the images to the applicable country. Once received, each country converts the images into a proprietary template and compares the data to the templates it has on file. Each country uses a different vendor to convert the images into a template and run the matching algorithm.

If a match is confirmed, the country that received the request will share the positive result as well as the demographic and other information about the individual.[70] With this information, the requesting country then determines next steps for the specific applicant—such as moving forward with the individual's visa or asylum application to enter the country or denying entry.

Technological and other key characteristics

Each country's database and administering agency is as follows:

- The Immigration and Asylum Fingerprint System in the U.K., administered by the U.K. Border Agency
- The Biometric Acquisition and Matching System in Australia, administered by the Department of Immigration and Citizenship
- The Automated Fingerprint Identification System in Canada, administered by the Royal Canadian Mounted Police for its own purposes and on behalf of Citizenship and Immigration Canada and the Canada Border Services Agency
- The IDENT System in the U.S., administered by DHS
- The Immigration New Zealand database

The raw fingerprint images meet ISO standards for quality and formatting. After assessing a match, each country deletes information received from another. This process ensures that no nation incorporates data from another country into its system.

Each country signs a formal protocol for bilateral, international data-sharing that outlines the requirements for privacy and security controls. DHS provides oversight to ensure compliance with the protocols, both within each country's database and through any process of exchange. The protocols include an agreement prohibiting the exchange of classified information, requiring two-factor authentication to access information, and mandating regular access audits.[71]

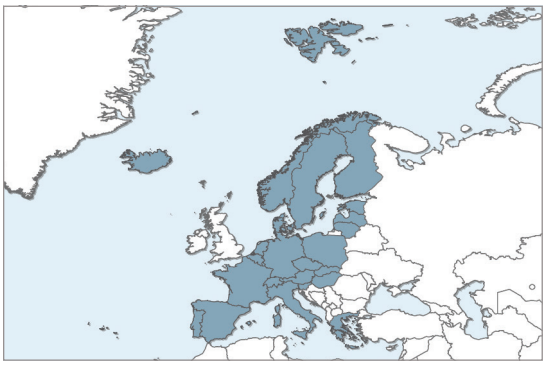
Lessons learned

The FCC Protocol allows disparate countries to access each other's biometric databases, highlighting three lessons for health care:

1. **Interoperability via a federated approach:** This federated data model lets each country maintain separate, centralized databases yet still query and share information among them. Because many health care organizations host their own database, this example demonstrates that a federated model connecting separate health care systems could allow for query-and-response messaging to perform patient matching using biometrics through the use of agreed-upon standards.
2. **Sharing raw images:** The exchange of raw images prevents vendor-lock. With raw images, users can maintain separate centralized databases, exchange raw images between them, select the biometric vendor of their choice, and use proprietary templates on which to run matching algorithms. This would allow health care organizations to select the system and vendor that meets their needs and still be able to exchange data with other facilities.
3. **Common agreement needed:** All the countries in the FCC Protocol agreed to a common set of policies addressing use, technical standards for storage and exchange, and privacy. In health care, a common agreement could set similar guidelines that develop standards and principles for the storing and sharing of biometrics. An existing model already exists in the United States: the Trusted Exchange Framework and Common Agreement (TEFCA). Congress in 2016 required ONC to establish TEFCA—an opt-in commitment for health information exchanges to use the same standards to receive and share health information. TEFCA

could outline modalities to use standards for images, requirements for exchange of those images, and privacy and security stipulations. Agreeing to a set of standards allows health care organizations to maintain their own systems and vendors, yet still be able to utilize a much larger connection of partners to improve the accuracy of patient matching.

eu-LISA Visa Information System



Location	Schengen area
Industry	Immigration/travel
Department/agency	European Union Agency for the Operational Management of Large-Scale IT Systems (eu-LISA)
Modality	Fingerprint
Use	Immigration
Storage	Centralized database

Officials of the Schengen area, which comprises 26 European countries, eliminated passport and border controls for travel within the region. Additionally, the Schengen area countries share biometric images for nonmember country visa applicants in order to create a greater level of security and reduce duplicative applications. A citizen from a non-Schengen area country can apply for a single Schengen visa and visit any member countries freely.

Schengen area countries use a shared database to manage visas, called the Visa Information System (VIS). The VIS uses biometrics to confirm the identity of visa applicants, avoid duplicative review among member countries, and reduce fraudulent applications. The system is managed by the European Union Agency for the Operational Management of Large-Scale IT Systems (eu-LISA), which manages all large-scale IT systems used for security and justice. The VIS also ensures that there are not duplicate visas for the Schengen area granted to the same person: for example, that a visa is not granted to the same individual by both Austria and Germany, when only a single Schengen visa is needed for visiting both countries.

At the end of 2017, the VIS contained data on more than 31 million visa applications, resulting in the granting of 29 million visas and the denial of 2 million across member countries.[72]

Workflow

The VIS contains all visa application data from Schengen area countries, including demographic information, digital photographs, and fingerprint images. When a traveler from outside the EU requires a visa to travel to a Schengen country, the individual goes to a consular office in his or her home country with a visa application and passport. The consular official collects the traveler's fingerprints and facial image, and the VIS stores the raw images along with the application.

At this point, the consular official determines if the traveler already received or applied for a visa, either to the same country or to another Schengen area country. To do this, the recently collected fingerprint images in the VIS are sent to the biometric matching system (BMS) that is also maintained by eu-LISA. BMS converts the images into templates in order to perform matching and never retains the raw images. BMS does retain the templates in order to use the images for future comparison. If the traveler already existed in the VIS from a prior visa, the consular official receives a match notification. The official then grants or denies the visa application.

If the visa is granted, a border control official collects the traveler's fingerprints again at an airport, seaport, or land crossing station. The fingerprint images are templated and run through the matching algorithm, and the border control official receives a yes or no response. If a match is confirmed, the traveler can proceed with the entry process. If there is no match, the border control official determines if the individual can enter the country

through an interview and a manual review of travel documentation and identification.

Technological and other key characteristics

Fingerprint images in the VIS meet the ANSI/NIST-ITL standard that determines quality, resolution, and size. All member states receive a fingerprint acquisition toolkit that performs quality control assessments on the collected fingerprints to ensure they meet the requirements and undergo processing by the biometric matching system.

As the VIS is a centralized database and all participating Schengen countries have access, users obtain access authorization and encrypt all data exchange over a private network.[73]

Visa applicants who visit frequently are not required to provide a new set of fingerprint scans with each application. Once stored, returning applicants can reuse their stored fingerprints for five years.[74]

Lessons learned

This example demonstrates how to share a centralized database across many users:

1. **Cooperation allows for shared infrastructure:** The VIS is shared by 26 countries with each nation collecting, storing, and querying data within it. Despite the geographic dispersion, each country adopted shared criteria, common standards, and a single process for managing visa applications to participate. If health care in the United States adopted a single system or multiple shared systems or services approach, organizations would also need to implement a similar common agreement—around principles, practices, and infrastructure—to effectively and securely exchange biometric data. If health care commits to a common agreement and infrastructure, it is feasible for multiple facilities to contribute to and reference a shared database to use biometrics for patient matching between organizations. As previously mentioned in the FCC Protocol example, TEFCA could serve as a platform to secure this cooperation.

Estonia national e-ID card

Location	Estonia
Industry	Government, public services, health care
Department/agency	Government of Estonia
Modality	Fingerprint (planned)
Use	Public services, health care
Storage	Decentralized

Estonia's e-ID card, introduced in 2002, is widely acknowledged as one of the most advanced approaches to digital identity and, although biometrics play a limited role, the infrastructure used offers lessons learned for health care. Estonia mandates an e-ID card for citizens over 15 years old. Citizens can use their e-ID as a national health insurance card, for official identification when traveling within the European Union, to remotely access their bank account, to pay for goods, to sign contracts, to view their health information, and even to vote.[75] Estonians can use e-IDs to access 99% of public services digitally—for instance, collecting social welfare benefits, paying for public transportation, or reporting a crime.[76] Currently, citizens set up a PIN to confirm identity when using their card, but Estonia is upgrading the system to allow for the use of a fingerprint in its place.

The e-ID is a physical card with an image of the citizen's face, basic demographic information, various security features, and a chip. The chip contains two digital certificates aligned to two separate PINs: one for identity authentication, and the other for providing a digital signature. Every individual's PIN stays the same (so long as the card is not stolen or breached in any way) and is used to confirm identity, access services, and send data.[77] By 2019 individuals had used the e-ID as a digital signature more than 900 million times, as well as to vote in national elections and electronically submit taxes.[78]

Despite the widespread use, Estonia dealt with a major breach in its e-ID and chip technology in 2017. The country recovered from this incident through risk mitigation strategies and transparent communication with the public. For example, cardholders could update their PIN remotely, and Estonia upgraded the card chips to address the cyber risk. The country resolved the crisis that same year as a result of cooperation among the government bodies, researchers, private sector partners, and residents.[79]

Workflow

The e-ID can be used to access many needed services and share information—including personal health information. Although biometrics are not yet a part of the process, the workflow includes elements relevant to health care in the United States that could integrate disparate health information and use digital identity in the confirmation of patients.

Estonia has an electronic health data repository (e-Health Record) that integrates data from providers and systems across the country. Acting as a centralized system, patients can view all of their health information in one place, regardless of the providers, facilities, or systems in which they received care. To access their data, patients use the e-ID to confirm their identity when logging in to the country's patient portal. Patients insert their e-ID into a COTS chip reader, and it reads their user credentials to log in to the portal. They then enter a PIN as a

security measure in order to access health information.

Through this process, patients also control access to their health information and determine which providers can view their complete e-Health record.[80] However, in a medical emergency, a provider uses a patient's e-ID card to view critical health information such as blood type, allergies, medications, and current diagnoses.[81] Similarly to accessing the patient portal, the provider can insert the e-ID into a chip reader to access basic emergency health information through e-Health Record.

If the e-ID card is lost or stolen, the individual must call the ID helpline within 24 hours so the following processes could be triggered:

1. **Certificates are suspended:** The individual must call the 24/7 helpline and identify themselves by stating their name and PIN. Suspending the certificates means that e-services cannot be accessed or used. To end the suspension, the individual must appear in person at a service point of the issuing authority and file an application to reactivate their e-ID.
2. **Revocation of e-ID/e-Residency card (including the certificates):** To revoke an e-ID, an individual must go to a service point and file an application. Revocation means that the certificates are revoked, and electronic functionality can neither be used nor turned back on.[82] The individual will need to reapply for a new e-ID.[83]

Technological and other key characteristics

The e-ID works across industries and sectors through the use of a solution called X-Road. X-Road securely shares information between systems and normalizes data. This system can send large data sets, write data into databases when appropriate, and search across multiple systems at the same time.[84] X-Road also provides an extra layer of security and ensures that only known and approved entities and users participate in the data exchange by monitoring and tracking access.

Estonia's e-Health Record displays relevant data in a patient portal. Providers and organizations can use an EHR and other systems of their choice, and those systems communicate directly with the central e-Health Record. Systems send information using standards-based interface messages (e.g., HL7 messages, the international standard for sending and receiving electronic health information, and DICOM, the standard for exchanging medical imaging data). In this case, the e-ID allows patients to authenticate their own identity and grant access to authorized users before viewing or sharing sensitive information. The card does not store health information.

The cards themselves work with most COTS scanners to read the chips. The chips store encrypted data that can be accessed only by an individual using a private PIN (and potentially biometrics in the future) or through a user granting access.

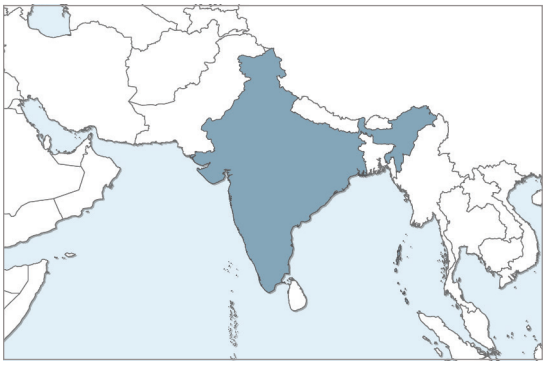
Lessons learned

The e-ID demonstrates that a digital identity can scale across many different industries, scenarios, and environments. Health care can apply these lessons:

1. **Risk mitigation strategies:** The crisis response in 2017 demonstrated that a breach doesn't need to result in the termination of the technology or its use. Having plans in place to address breaches, maintaining open communication on resolution and next steps, and getting a fix out as quickly as possible allowed the e-ID card to remain a trusted solution. In health care, a similar risk mitigation and communication plan is needed to address potential breaches to the selected technology.
2. **Identity can be repurposed:** The e-ID's use and purpose grew exponentially beyond identity confirmation. As discussed, Estonian citizens can use the e-ID to vote, as proof of health insurance, and as a digital signature, among other purposes. A similar digital identity approach for a patient in the U.S. could be used

for initial identity confirmation and also for other health purposes, such as checking in for an appointment, telehealth access, or filling a prescription. The digital identity could include biometrics as part of it—in place of a PIN—and individuals could opt in to their use in health care for patient matching and other purposes.

India's Aadhaar program



Location	India
Industry	Public services
Department/agency	Government of India
Modality	Fingerprint, iris, facial scan
Use	Public services
Storage	Centralized database

India's Aadhaar program is the world's most extensive use of biometrics: More than 1.2 billion people have registered and received an Aadhaar number.[85] This optional number allows both citizens and noncitizens who reside in India to use multiple biometric modalities to identify themselves when receiving social services, traveling, or opening a bank account. The Aadhaar program collects fingerprints, iris scans, and a digital photograph alongside demographic information.

Any individual, regardless of age, can opt in to the program and receive a 12-digit Aadhaar number after completing the registration process. Individuals can use the number to obtain public services and benefits and confirm identity within the private sector, such as when applying for a job.

Prior to the Aadhaar program, nearly 400 million Indian citizens did not have a way to prove their identity.[86] The Unique Identification Authority of India (UIDAI) implemented the voluntary Aadhaar initiative in 2009 as a way for citizens to have a government-sponsored method to confirm their identity.

Despite being lauded for its efficiency and cost-savings, the program has also received criticism about the danger of compromising individuals' data in the event of a breach, because it collects all biometric modalities (face, finger, and iris).[87] The program further raised questions of inequity: Individuals with medical conditions such as leprosy may not be able to take part in the program because their condition prevents them from providing fingerprints or iris scans. Due to these concerns, the Indian Supreme Court found that private companies could not require the use of the Aadhaar number (though individuals can still choose to use their Aadhaar number to confirm identity for private sector services).[88]

Workflow

To receive an Aadhaar number, an individual goes to an official enrollment center, which are located across the country. The registration process requires providing demographic information, a verified government-issued ID (e.g., a birth certificate or driver's license), and biometric information: 10 fingerprints, iris scans, and a facial photograph.[89] In situations where individuals do not have supporting documentation or a government-issued ID, they can work with someone who the Indian government has called an "introducer"—an individual who has a verified identity and is a recognized member of the community, such as an elected official, teacher, or health care worker.[90] An introducer can vouch for an individual's identity in lieu of providing supporting documentation.

At the enrollment center, an operator scans the documents, returns them to the resident, and manually enters the demographic data. The operator then collects the biometrics. For children under 5 years old, only a facial image is

captured along with one parent's biometric confirmation.[91] For residents over 5 years, all three modalities are captured.[92]

The government then stores the raw images in a central database called the Central Identities Data Repository (CIDR). The raw images are sent to biometric service providers, where they are converted to proprietary templates in order to be used for matching in the future. India uses three different biometric service providers to offer options for using different organizations to conduct the matching—each with its own templates. Each biometric service provider stores only its proprietary templates and deletes the images once processed. This step completes the enrollment process.

Then, individuals can use their Aadhaar identifier at service providers, such as government departments or private organizations. These service providers go through a certification process and must use registered biometric devices.[93] They collect and use biometrics in real time to confirm identity, which occurs through a multistep process:

1. An individual provides their Aadhaar number and has a biometric modality scanned.
2. The technology used by the service provider sends the image to a biometric service provider, where it is converted into a proprietary template.
3. The biometric service provider already has templates of the biometric provided at Aadhaar enrollment and runs a matching algorithm comparing those to the newly captured biometric.
4. The biometric service provider informs the service provider if the biometric matches the Aadhaar number. If a match occurs, the individual can obtain the service.

Technological and other key characteristics

All biometric images collected for Aadhaar meet ISO standards.[94] These standards dictate the format of the collected image, including resolution, content, and size.

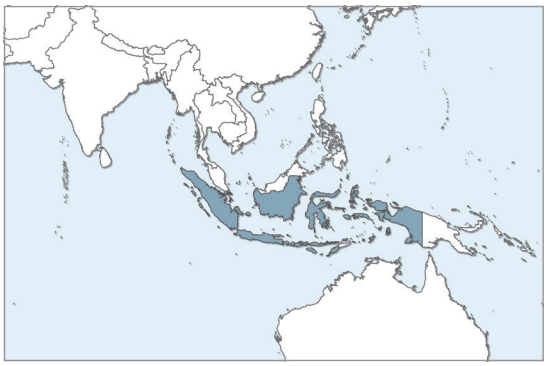
As the CIDR contains and sends sensitive information, all data is encrypted in transit. Anti-tampering measures are used to safeguard data.[95] The system tracks all actions, and the government orders regular audits. The authentication requests to the CIDR are purged every six months.[96] Further, the program remains voluntary, and private entities cannot require the use of Aadhaar numbers to confirm an individual's identity.

Lessons learned

This use case demonstrates some challenges with large-scale biometric deployment and the utility of raw images for interoperability:

1. **Biometrics can highlight inequities:** Just as artificial intelligence and machine learning have brought to light existing inequities in health care, the use of biometrics can present similar challenges. Biometric use can, for example, present obstacles for individuals who cannot provide fingerprints or iris scans due to existing health conditions. Similarly, facial scanning technology may not accurately identify people of color.[97] This case serves as a reminder that no single modality or approach can work universally for identity confirmation and that software should be designed with inclusivity in mind. Health care should consider solutions that address these gaps and also have backup authentication options, such as texting a smartphone with a unique code.
2. **Raw images allow for interoperability:** The secure sharing of raw images in Aadhaar allowed for the use of multiple vendors without sacrificing interoperability. The sharing of images allows new facilities and systems to opt in to the biometric infrastructure over time, as the solution becomes more commonplace and patients are comfortable with its use—all while allowing organizations to choose biometric vendors that meet their needs.

ID2020



Location	Indonesia
Industry	Public services
Department/agency	Indonesian government (pilot)
Modality	Fingerprint, facial scan
Use	Digital identification
Storage	Decentralized

The need for digital identity is high in rural and hard-to-reach areas and in countries with high percentages of displaced populations, where many individuals do not have a government-issued form of identification. ID2020, a nongovernmental organization, works across the public and private sectors to develop new models for using digital identification around the world.

Individuals store this digital identity, including biometrics, on a smartphone application. By using this approach to demonstrate their identity, people can receive needed vaccinations, apply for a job, open a bank account, receive government services, and vote. This solution puts users in control of their identification information; they can decide with whom and for what purpose to share data.

ID2020 launched several pilot programs that use a smartphone application to store a digital identity. For example, in Indonesia, local governments used smartphone-driven digital identity to more accurately distribute state-subsidized propane gas; the details of that pilot are the focus of this use case.

Although the Indonesian pilot is a simple workflow, it raised several important considerations for future use. The program noted that in regions where local government was more engaged in the project and in communicating with individuals, it received higher numbers of volunteers for participation, compared to other regions where government was less engaged.[98] The program also dealt with challenges collecting biometrics, including dust and dirt obstructing clean fingerprint reads, headscarves and veils worn by women that caused issues with facial recognition software, and network connectivity affecting collection and matching, especially in more rural and remote areas.[99] Although the pilot did not solve all of these problems, it provided information on how to improve software and infrastructure to work in remote areas and across all populations.

In the spring of 2020, the media highlighted criticism that ID2020 would be used to track individuals through microchipping to combat the global coronavirus pandemic.[100] However, neither the digital identity solution nor any of the pilot programs use microchipping or location tracking. The digital identification system still carries possible risks to privacy and security—as was illustrated with prior examples—that are mitigated through user-driven storage and access.

Workflow

Indonesia recently completed a pilot program in 2019 of approximately 6,000 households within several different rural communities that used digital identity to access and receive government subsidies for liquified propane gas.

In Indonesia, local governments had challenges ensuring subsidized propane went to the correct person. In

an effort to stop fraud and confirm that only qualified individuals were receiving the subsidized price, they implemented this pilot to use a confirmed digital identity. The National Team for the Acceleration of Poverty Reduction, an Indonesian cross-agency collaboration formed to improve implementation of social welfare programs and reduce inequity,[101] estimated that better oversight could save the Indonesian government up to $3.49 billion per year.[102]

To enroll, individuals go to a registration center, where an official collects and confirms a government-issued form of identification (if one exists), demographic information, and biometrics, which include fingerprints and a digital photograph. These biometric images are stored on the individual's smartphone. Within an application on the smartphone, an individual can create and store a digital identity using the demographic information and the biometric images. After enrollment, the person can use the digital identity app, along with biometric confirmation, as proof of identity and to receive the subsidized price.

When purchasing propane from a local authority, the individual opens the smartphone digital identity app containing their digital identity and an official scans a QR code within the app. Then, the official collects fingerprints using a digital scanner and/or a facial image with a digital or smartphone camera. The images are sent to a remote biometric processing and matching system, where they are converted to templates. The biometric system then confirms a match between the image stored on the smartphone and the one just taken by the official. The match confirmation enables the individual to purchase propane at a subsidized price.[103]

This pilot program is a single representation of how smartphones, in concert with biometrics, could improve access to services, reduce fraud, and ensure every individual has access to a validated form of identification. Several different pilots around the world have demonstrated the ID2020 approach, albeit with workflow changes because they are context-dependent.

Technological and other key characteristics

ID2020 uses a decentralized, distributed database architecture and a multimodality solution. In this model, sensitive data, including raw images, are saved only on a user's smartphone in an application and can be shared only by the individual granting access. No central database stores the images or templates.

A multimodality system is another feature of ID2020's approach. Collecting and using fingerprints, facial images, and iris scans provides multiple forms of biometrics and backups if one method fails or is unreliable. This also helps avoid issues such as those that the Indonesian pilot experienced, where fingerprints were unreadable because of dust or dirt.

All biometric images collected adhere to ISO standards, which dictate the quality of characteristics of the image, such as resolution, color, and format. The use of standards helps support exchange as pilot projects evaluate its use for identity between different types of systems and authorities.

Lessons learned

Although ID2020 has a wide range of possible uses, the following two lessons are the most applicable to health care:

1. **The use of personal devices:** Mobile technology is available worldwide and has reached even the most remote populations. ID2020 chose mobile applications because it found that even displaced refugees who did not have access to identity records still often had access to personal devices.[104] In a 2016 consumer study of adult smartphone users, nearly 70% of respondents said that they want apps that provide digital identity documents, such as passports and national IDs.[105] Health care in the United States could also leverage this approach for individuals to proactively share their digital identity with health care providers to support matching. Patients could use a smartphone application that collects demographic information, verifies a

government-issued ID, and collects facial images to confirm identity. This process meets NIST's identity-proofing standards and is managed by the patient.[106] Biometrics are incorporated within the digital identity, as within the Indonesian example, and could be used across health care facilities to confirm patient identity.

2. **Infrastructure needs:** As the Indonesian pilot demonstrated, individuals in rural and remote areas also require access to services. However, these areas faced challenges with connectivity, which were especially apparent when it came to exchanging data required for biometric matching. For these solutions to be equitable and accessible across the United States, infrastructure and connectivity issues must be addressed. Broadband remains inaccessible to portions of the country, and these areas may not yet have the infrastructure needed to support a biometrics-based solution for patient matching that relies on this type of connectivity.[107]

Overarching themes to apply to the U.S. health care system

Health care can apply lessons learned from these examples in determining how to use biometrics for patient matching between organizations. Across the examples, eight main themes emerged:

- *Barriers and concerns about implementing biometric solutions remain.*
- *Recent innovations make deployment easier.*
- *Site- and person-centric approaches are emerging.*
- *Raw images are used for interoperability.*
- *Standards are necessary.*
- *Perceived benefits in convenience outweigh privacy issues.*
- *Opportunities exist for mitigating privacy concerns.*
- *Government involvement can encourage adoption and adherence to standards.*

These themes address possible solutions to challenges—such as privacy, security, equity, interoperability, and consent—and how other industries designed and oversee the data exchange infrastructure. Additionally, the importance of governance—such as standards and compliance—cut across each of the aforementioned themes.

Theme 1: Barriers and concerns about implementing biometric solutions remain

As with any technological solution, health care should always consider pertinent challenges and the gaps they may expose. Unwittingly, biometrics could further perpetuate inequities in health care. Despite recent advances, certain modalities and associated algorithms do not work equitably across populations. There are religious and cultural sensitivities that could prevent an individual from submitting or capturing a facial image. In the ID2020 implementation in Indonesia, facial recognition faced challenges when women wore headscarves in the captured images.[108] Health care would also need to find ways to implement solutions and policies that meet the needs of pediatric populations. This could include more frequent collection of images as features and characteristics change with age or allowing parents to provide consent to collect biometrics until the patient reaches a specified age. Further, individuals with dermatological conditions such as eczema cannot provide digital fingerprints that would work in an indexing system. Similarly, those missing digits or those who have degenerative conditions would also require alternative options.[109]

Specific challenges with the technology also need to be addressed and understood. For example, algorithms for facial recognition struggle to correctly identify women as well as people of color.[110] Further, facial images could be collected and used without the knowledge of the individual, challenging traditional notions of privacy and consent.[111] Even when algorithms are adjusted and tuned to changes in population size, distribution, and diversity, existing biases could affect care—such as withholding pain management care based on an individual's race.[112] Other industries compensated for these inequities by collecting multiple modalities and through continuous assessment and updates of the algorithms and biometric systems. More inclusive products, developed by a diverse workforce, have the potential to advance, rather than inhibit, health equity. Engaging health equity experts alongside facial recognition and technical professionals could help lead to the implementation of more equitable and privacy-preserving solutions.

It is important for users to invest in foundational infrastructure that allows biometric solutions to be nationally accessible and scalable. Several examples highlighted challenges with system delays because of network connectivity, slowness in uploading images, and access issues in remote communities. The U.S. struggles with

broadband access and network connectivity, both in rural areas (because of a lack) and in highly concentrated urban areas (because of volume).[113] Prior to a national-level implementation of biometrics, health care may need to upgrade infrastructure and address issues of network access.

Theme 2: Recent innovations make deployment easier

Recent advances in technology allow personal devices to collect biometrics, leading to similar innovations that make national deployment of a biometric solution more feasible. Smartphones, tablets, COTS cameras and scanners, and embedded chip technology all can collect and store biometric images and digital identities, creating an opportunity for easier—and more affordable—deployment. Many examples, such as the use of two-factor authentication for EPCS, the KTDI travel program, and ID2020, highlighted the use of a smartphone or COTS technology to collect biometric images. Webcams and tablets can take facial images that meet NIST standards (as demonstrated in the CBP Biometric Exit program), smartphone apps can store digital identities, and embedded chips on credit cards house encrypted biometric templates. These more affordable technologies increase accessibility, making it feasible for smaller health care facilities to implement biometrics.

Often, those facilities use these technologies already for other reasons—such as checking patients in, creating patient portal accounts, or using apps to assist with care management—and thus they could be repurposed. Additionally, many places of care today already collect patient photos using digital cameras or tablets for manual identity confirmation.[114] Providers sometimes use images for diagnosing certain clinical conditions, such as genetic disorders.[115] Facilities could use these existing images to support patient matching. This approach would not add new workflow procedures to capture the photo but would require some technological adjustments to use the information for cross-organization matching.

Further, cards with embedded chips, such as those used in Estonia, could replace health insurance cards, with the chip containing a biometric template, such as a fingerprint, allowing for easy identity confirmation. Given the variety of available technologies and systems, health care organizations could choose their own vendors, devices, and methodologies for collecting and using biometrics, yet still achieve interoperability with adherence to standards for images and exchange.

Theme 3: Site- and person-centric approaches are emerging

Although biometric implementations have traditionally focused on the use of capital equipment purchased and used by facilities, the near ubiquitous emergence of smartphones introduces patient-centric approaches. Given that smartphones and other mobile devices (such as iPads or other tablets) can take images that meet NIST standards, patients could play an active role in capturing facial images and managing their personal biometrics.

Although some solutions still require in-house technology and systems—such as chip readers, fingerprint or palm scanners, and centralized databases for storing images—the proliferation of cases that work with personal devices means that even patients living in remote or less affluent areas of the country can use biometrics. The ID2020 example in Indonesia used a smartphone app-based process because of widespread use; even displaced refugees, who often had no form of government identification, still had access to some form of personal device.[116]

In health care, patients often use smartphones to access portals with their health information and to use apps that help with disease management. Patients could also use smartphones to provide a facial image or a fingerprint to a health care facility so that the biometric image becomes part of their health record, just as providers did in the EPCS example. Similar to how facilities exchange demographic information for patient matching, biometric images could be shared as a component used for matching. Smartphone apps, similar to the KTDI example, could allow patients to provide consent and grant appropriate access to health information.

Theme 4: Raw images are used for interoperability

Matching across systems and databases requires either the exchange of raw images or a common template. Many of the examples—the CBP Biometric Exit, FCC Protocol, and eu-LISA system, particularly—demonstrated cooperation across government agencies and even across countries; in order for participants to share information, they exchanged raw images. Once the recipient received the raw image, it was converted into a proprietary template in order to run the matching algorithm. The sharing of images ensured interoperability across technologies and locations.

Organizations used encryption, data retention policies, access restrictions, and audits to address the associated security concerns with exchanging raw images. Although these efforts mitigated concerns, they did not eliminate them. Health care should weigh concerns with exchanging raw images against the interoperability benefits and develop sufficient privacy and security solutions to protect the information.

Rather than sharing raw images, another option that allows for interoperability is developing and using a standard template for each modality. Currently, an ISO standard template exists for fingerprints, but not for other modalities.[117] Working with ISO and NIST to create a standard for other modalities would allow health care to exchange these templates across organizations, rather than a raw image. However, to be interoperable, all biometric systems and vendors would need to agree to and develop products in line with these standards. Further, if all vendors agreed to a standard template, it would be public—meaning that the template standard could be found easily and used nefariously in breaches or attacks. A public, standard template would confer limited—if any—protections beyond raw images.

Theme 5: Standards are necessary

Although standards for templates of all biometric modalities do not yet exist, they do for images. Standards for images of biometric modalities used in all examples (facial images, fingerprints, iris scans, and palms) exist through NIST/ANSI that determine details such as the image quality and the specifications for formatting. NIST/ANSI also developed a standard message for how to exchange and share biometric images between systems.[118]

All examples adhered to image standards; meeting these ensured that the image quality is high enough for template conversion and for running a matching algorithm. Further, adherence to standards allows organizations to exchange raw images among systems. Using the standard message for exchange lets different organizations, agencies, and countries share images.[119] Regardless of the method health care chooses for exchange—raw images or standard templates—using standards for the collected modalities remains essential.

However the health care industry implements biometrics, the necessary standards could be appended to the United States Core Data for Interoperability (USCDI). This is a required set of data elements, including demographic information such as names and addresses but also certain medical information, that EHRs must make available in a standard manner. Inclusion in the USCDI would ensure all health IT products certified to federal standards contain uniform functionality for collecting and sharing standard biometric data.

Theme 6: Perceived benefits in convenience outweigh privacy issues

Individuals opt in to using biometric solutions that make their lives easier. Across the travel-related and identity-confirmation examples, users chose the biometric option when weighing other concerns, including security of personal data, often because the biometric option reduced wait times. Travelers must choose to create mobile passports to board planes and pass through customs with a smartphone app and facial recognition, rather than manual review of a physical passport and other travel documents. In several examples, users chose to create and use digital identities to access government services, rather than using manual processes (for example, showing

proof of address with utility bills or government-issued ID) to confirm identity. Once created and confirmed, individuals could use their digital identity with only their smartphone. The choice that individuals made to use biometric options over others demonstrates the willingness to opt in to solutions that gain efficiency.

In past patient focus groups conducted by Pew, many individuals stated their preference for a solution for matching that didn't involve a card or a number.[120] Further statements expressed a desire for a solution that could be used while an individual is unconscious, or otherwise in an emergency situation.[121] Biometrics could help meet these patient preferences and therefore offer solutions to make their lives easier.

For the ease of use to outweigh privacy concerns, many industries allow individuals to grant and audit access to their personal data. For international travel, individuals could determine if they planned to use a mobile passport and then share their passport information—including a facial image—through the app on their smartphone with airport and airline officials. Personal data could not be accessed without the individual granting it.

In other examples of digital identity, users act as the auditor of their own data. Individuals can retroactively review any access to their data to understand who reviewed information and when. Applications also let users remove consent, terminating previously permitted access. Giving individuals ultimate control over their own data, including the ability to grant, audit, restrict, and remove access, could help mitigate privacy concerns. Health care could similarly use apps and smart phones to streamline patient consent, as well as for individuals to control access to and use of their personal health information.

Theme 7: Opportunities exist for mitigating privacy concerns

Privacy and security concerns associated with using biometrics are not specific to health care. The industries in the examples understood the risks that came with collecting, storing, and sharing biometric images and templates. Although no single solution can promise protection from all breaches or attacks, the examples demonstrated that multiple strategies used in conjunction can mitigate threats.

For those examples that used centralized databases, organizations employed armed security guards; limited physical access to facilities; allowed only authorized users and required dual authentication to search and view data; held frequent audits; and used encryption to secure sensitive data. Others gave the individual control over their own data, and the user could grant, revoke, and review access. All examples encrypted data at exchange, including for sharing raw images. Access to data was always limited to ensure that officials only had the access needed to carry out essential job functions; these organizations also conducted frequent audits.

As the Estonian e-ID example demonstrated, even with protections in place, breaches occur. However, because Estonia had risk mitigation plans and invested users, the country quickly addressed the breach, had open channels of communication with citizens, and pushed out a technical fix to every national e-ID card. Despite this threat, citizens continued using their e-IDs; Estonians' access to digital tools and services through their e-ID became an expected way of life.[122]

Because health care data is sensitive and already enjoys some protections, users who access this information are regulated and audited. Similar protections could be implemented in a biometric-based system and may already confer from existing policies, such as those implementing HIPAA. In addition, health care already adheres to policies and procedures for HIPAA violations and inappropriate access to data; these same approaches may transfer to biometric data.

Further, state and national regulations and legislation could address breaches to biometric data as well. The European Union addresses biometric data in the General Data Protection Regulation, but there is no similar national-level law in the U.S.[123] Several states (Illinois, Texas, Washington, and California) passed legislation

regulating the collection, use, and retention of biometric data.[124] Updating privacy law, either at the state or federal level, could provide further protections for the use of biometric data in health care.

Theme 8: Government involvement can encourage adoption and adherence to standards

Particularly because biometrics come with multiple decision points—modality, format, and storage—government involvement could set standards and determine the foundational elements necessary for implementing an interoperable, equitable, and secure biometrics solution. For example, using existing standards, from NIST and ISO, and providing a forum to determine a cooperative agreement that outlined privacy, security, and anti-discrimination protections could help health care begin to understand how to design and implement a biometrics solution to enhance patient matching. The FCC Protocol and the eu-LISA system illustrate how cooperation around a set of standards and policies can provide guidance without sacrificing flexibility.

ONC, with other government agencies, has demonstrated how incentives and the creation of standards can encourage adoption of and adherence to technological solutions. USCDI is an example of a government-mandated specification created to ensure common and necessary data elements are exchanged between health care providers and facilities, regardless of the system in place. Additionally, TEFCA demonstrates how a national collaboration and public-private partnerships can create common approaches and agreements on data exchange.

Conclusion

The use of biometrics in industries around the world provides valuable insight for implementing any solution to resolve one of the most persistent and vexing problems in health care: patient matching. Building on the lessons learned from these applications, patients, the health care industry, and policymakers can weigh concerns against benefits and make informed decisions about the best methods and strategies for integrating biometrics.

This technology can help providers and patients have more complete and accurate health information to inform treatment decisions when used as part of a larger solution for patient matching. With collaborative, cross-sector leadership, health care can design a system incorporating biometrics that prioritizes both interoperability and privacy while working to better link records across different sites of care.

Appendix I: Examples considered

Use case	Cross-entity	Geography	Industry	Technology	Modality	Rationale
CBP Biometric Exit	Yes	U.S.	Travel	Centralized	Face	Provides lessons learned from a security and privacy perspective.
KTDI	Yes	Canada, Netherlands	Travel	Decentralized	Face	Decentralized example with emphasis on innovation to inform future possibilities for health.
Mastercard	No	Global	Financial services	Centralized	Fingerprint (FP)	Unique technology with capture and match on card.
ID.me and Allscripts	Yes	U.S.	Health	Centralized	Face	Innovation in facial recognition and self-service mobile capabilities.
DHS US-VISIT	Yes	U.S.	Government/ travel	Centralized	FP (limited face, iris)	Large-scale implementation, multimodality and 60 agencies involved.
Five Country Conference Protocol	Yes	U.S., Canada, U.K., New Zealand, Australia	Public safety	Federated	FP	High complexity in sharing sensitive data across entities with different privacy and security requirements.
eu-LISA biometric matching	Yes	Schengen area	Public safety	Centralized	FP	Cross-entity use with large expansion between countries and across borders.
Estonia national e-ID	Yes	Estonia	Government	Centralized	PIN	Uses Xroad, which is an integration architecture that enables data-sharing across disparate entities.
India's Aadhaar program	Yes	India	Government/ public services	Centralized	Face, FP, iris	One of the most prominent biometric use cases. Largest database in the world.
ID2020	Yes	Developing countries	Government/ public services	Decentralized	FP, face	Similar to KTDI, has direct application in health care, decentralized architecture.

The examples listed below were researched and considered but not selected because of one or several of the following reasons: too early in implementation stages to have lessons learned, not enough publicly available data, or too similar to already-selected examples.

- Clear: digital identification in travel
- Next Generation Identification (NGI) Rap Back service: FBI
- Iris scanning in health care facilities in South Africa
- Imprivata and Community Health: patient identification within an organization
- Neurotechnology Somaliland National ID project
- NEC Corporation of America and VidyoCloud video-enabled applications
- United Nations High Commissioner for Refugees (UNHCR) Biometric Identity Management System (BIMS)
- Schiphol Airport Automated Border Clearance
- Transportation Security Administration (TSA) Technology Infrastructure Modernization program (TIM)
- Mexico Tax Agency multibiometric enrollment system
- Gemalto and the European Asylum Dactyloscopy Database (EURODAC)
- Fulcrum Biometrics Homeless Services Management System
- Ping An: customer service with biometrics
- Princeton Identity: senior living facility
- Auburn University
- IrisGuard and Patientory
- Patient biometric data in Ghana
- SimPrints: developing country vaccinations

Endnotes

1 The United States National Library of Medicine, "Visible Proofs: Forensic Views of the Body," accessed June 5, 2020, https://www.nlm.nih.gov/exhibition/visibleproofs/galleries/technologies/bertillon.html; F. Galton, *Finger Prints* (London: Macmillan, 1892).

2 L.A. Hutchins, "Chapter 5: Systems of Friction Ridge," in *The Fingerprint Sourcebook* (Washington, D.C.: U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, 2011), https://www.ncjrs.gov/pdffiles1/nij/225325.pdf.

3 The National Science and Technology Council, "Biometrics in Government Post-9/11" (2008), https://fas.org/irp/eprint/biometrics.pdf.

4 Federal Bureau of Investigation, "Biometric Center of Excellence (BCOE)—Modalities," accessed July 16, 2020, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/biometric-center-of-excellence-1/modalities-1.

5 Biometrics Institute, "Types of Biometrics," accessed June 5, 2020, https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/.

6 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/.

7 Federal Bureau of Investigation, "Biometric Center of Excellence (BCOE)—Modalities."

8 National Institute of Standards and Technology, "ANSI/NIST-ITL Standard," accessed June 5, 2020, https://fingerprint.nist.gov/standard/.

9 Sarfraz, "Adermatoglyphia."

10 Federal Bureau of Investigation, "Biometric Center of Excellence (BCOE)—Modalities."

11 Ibid.

12 Ibid.

13 STAT, "The Fight Over Facial Recognition Technology Gets Fiercer During the Covid-19 Pandemic," May 5, 2020, https://www.statnews.com/2020/05/05/facial-recognition-technology-covid19-tracking-california-bill/.

14 F.W. Wheeler, X. Liu, and P.H. Tu, "Face Recognition at a Distance," in *Handbook of Face Recognition,* eds. S. Li and A. Jain (London: Springer, 2011), https://link.springer.com/chapter/10.1007/978-0-85729-932-1_14#citeas.

15 P. Grother, M. Ngan, and K. Hanaoka, "NISTIR 8280: Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects" (National Institute of Standards and Technology, 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

16 The Verge, "IBM Will No Longer Offer, Develop, or Research Facial Recognition Technology," June 8, 2020, https://www.theverge.com/2020/6/8/21284683/ibm-no-longer-general-purpose-facial-recognition-analysis-software.

17 S. Dargan and M. Kumar, "A Comprehensive Survey on the Biometric Recognition Systems Based on Physiological and Behavioral Modalities," *Expert Systems With Applications* 143 (2020), https://www.sciencedirect.com/science/article/pii/S0957417419308310.

18 Grother, Ngan, and Hanaoka, "NISTIR 8280."

19 Dargan and Kumar, "A Comprehensive Survey on the Biometric Recognition Systems."

20 Federal Bureau of Investigation, "Biometric Center of Excellence (BCOE)—Modalities."

21 Dargan and Kumar, "A Comprehensive Survey on the Biometric Recognition Systems."

22 Ibid.

23 Federal Bureau of Investigation, "Biometric Center of Excellence (BCOE)—Modalities."

24 National Institute of Standards and Technology, "About NIST," accessed Oct. 21, 2020, https://www.nist.gov/about-nist.

25 International Organization for Standardization, "About Us," accessed Oct. 21, 2020, https://www.iso.org/about-us.html.

26 National Institute of Standards and Technology, "Glossary—Decentralized Network," accessed Oct. 21, 2020, https://csrc.nist.gov/glossary/term/Decentralized_network.

27 National Institute of Standards and Technology, "Glossary—Centralized Network," accessed Oct. 21, 2020, https://csrc.nist.gov/glossary/term/Centralized_network.

28 National Institute of Standards and Technology, "Glossary—Federation," accessed Oct. 21, 2020, https://csrc.nist.gov/glossary/term/federation.

29 The Pew Charitable Trusts, "Enhanced Patient Matching Is Critical to Achieving Full Promise of Digital Health Records," accessed April 30, 2020, https://www.pewtrusts.org/en/research-and-analysis/reports/2018/10/02/enhanced-patient-matching-critical-to-achieving-full-promise-of-digital-health-records.

30 Ibid.

31 Ibid.

32 Fierce Healthcare, "Sen. Rand Paul Continues Fight Against Patient Identifier, Introduces Bill to Overturn Authority Under HIPAA," Sept. 26, 2019, https://www.fiercehealthcare.com/tech/sen-rand-paul-continues-fight-against-national-patient-identifier-introduces-bill-to-overturn.

33 Modern Healthcare, "House Votes to Overturn Ban on National Patient Identifier," June 13, 2019, https://www.modernhealthcare.com/politics-policy/house-votes-overturn-ban-national-patient-identifier.

34 Departments of Labor, Health and Human Services, and Education, and Related Agencies Appropriations Act, HR 1865 (2020), https://appropriations.house.gov/sites/democrats.appropriations.house.gov/files/HR%201865%20-%20Division%20A%20-%20LHHS%20SOM%20FY20.pdf

35 The Office of the National Coordinator for Health Information Technology, "2015 Update to Congress on the Adoption of Health Information Technology" (2016), https://dashboard.healthit.gov/report-to-congress/2015-update-adoption-health-information-technology-full-text.php#progress-update.

36 The Pew Charitable Trusts, "Patients Want Better Record-Matching Across Electronic Health Systems" (2018), https://www.pewtrusts.org/en/research-and-analysis/issue-briefs/2018/10/patients-want-better-record-matching-across-electronic-health-systems.

37 National Academies of Sciences Engineering and Medicine et al., "2 - the State of Health Disparities in the United States," in *Communities in Action: Pathways to Health Equity*, eds. J.N. Weinstein et al. (Washington, D.C.: National Academies Press, 2017), https://www.ncbi.nlm.nih.gov/books/NBK425844/.

38 Healthcare IT News, "Biometrics Entering a New Era in Healthcare," July 30, 2018, https://www.healthcareitnews.com/news/biometrics-entering-new-era-healthcare.

39 Federal Communications Commission, "Mapping Broadband Health in America," accessed June 5, 2020, https://www.fcc.gov/health/maps.

40 U.S. Customs and Border Protection, "Biometric Breakthrough: How CBP Is Meeting Its Mandate and Keeping America Safe," accessed June 5, 2020, https://www.cbp.gov/frontline/cbp-biometric-testing.

41 U.S. Department of Homeland Security, "DHS/CBP/PIA-056 Traveler Verification Service," last modified Jan. 9, 2020, https://www.dhs.gov/publication/dhscbppia-056-traveler-verification-service.

42 Office of Inspector General, Department of Homeland Security, "Progress Made, but CBP Faces Challenges Implementing a Biometric Capability to Track Air Passenger Departures Nationwide" (2018), https://www.oig.dhs.gov/sites/default/files/assets/2018-09/OIG-18-80-Sep18.pdf.

43 U.S. Department of Homeland Security, "DHS/CBP/PIA-056 Traveler Verification Service."

44 Ibid.

45 Known Traveller Digital Identity, accessed June 5, 2020, https://ktdi.org/.

46 D. Bachenheimer (principal director, Accenture), interview with The Pew Charitable Trusts, Feb. 14, 2019.

47 Biometric Update, "Mastercard and Orange: Why Global Brands Are Delving Into African Biometrics," June 28, 2019, https://www.biometricupdate.com/201906/mastercard-and-orange-why-global-brands-are-delving-into-african-biometrics.

48 Mastercard, "Pointing the Finger at Biometric Card Misconceptions," Mastercard, accessed July 18, 2019, https://newsroom.mastercard.com/2018/10/08/pointing-the-finger-at-biometric-card-misconceptions/.

49 ID.me, "Identity Gateway," accessed July 2, 2019, https://www.id.me/business/identity-gateway.

50 ID.me, "Electronic Prescription of Controlled Substances (EPCS) Provider Credentialing," accessed July 18, 2019, https://www.id.me/business/epcs.

51 ID.me, "Terms of Service, Version: 8.7.2," accessed July 18, 2019, https://www.id.me/terms.

52 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.

53 J. Mafera (head of product, Tausight), interview with The Pew Charitable Trusts, Feb. 14, 2019.

54 B. Hall (founder and CEO, ID.me), interview with The Pew Charitable Trusts, Feb. 14, 2019.

55 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.

56 The White House, "National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy" (2011), https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

57 K. Megas et al., "NISTIR 8054 NSTIC Pilots: Catalyzing the Identity Ecosystem" (National Institute of Standards and Technology, 2015), https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8054.pdf.

58 Thales Group, "DHS' Automated Biometric Identification System IDENT—The Heart of Biometric Visitor Identification in the USA," accessed June 5, 2020, https://www.gemalto.com/govt/customer-cases/ident-automated-biometric-identification-system.

59 Ibid.

60 Ibid.

61 Ibid.

62 AFCEA, "Congress Raises Privacy and Civil Liberty Concerns With the DHS' Use of Biometrics," Signal, July 11, 2019, https://www.afcea.org/content/congress-raises-privacy-and-civil-liberty-concerns-dhs%E2%80%99-use-biometrics.

63 U.S. Customs and Border Protection, "CBP Meets With Privacy Groups to Discuss Biometric Exit," news release, Feb. 2, 2018, https://www.cbp.gov/newsroom/national-media-release/cbp-meets-privacy-groups-discuss-biometric-exit-0.

64 U.S. Department of Homeland Security, "Biometric Standards Requirements for US-VISIT Version 1.0" (2010), www.dhs.gov/xlibrary/assets/usvisit/usvisit_biometric_standards.pdf.

65 U.S Department of Homeland Security, "DHS/OBIM/PIA-001 Automated Biometric Identification System," accessed July 17, 2020, https://www.dhs.gov/publication/dhsnppdpia-002-automated-biometric-identification-system.

66 Biometric Update, "Inside the HART of the DHS Office of Biometric Identity Management," accessed June 5, 2020, https://www.biometricupdate.com/201809/inside-the-hart-of-the-dhs-office-of-biometric-identity-management.

67 U.S. Department of Homeland Security, "Privacy Impact Assessment for the US-VISIT Five Country Joint Enrollment and Information-Sharing Project (FCC)" (2009), https://www.dhs.gov/sites/default/files/publications/privacy_pia_usvisit_fcc_0.pdf

68 Home Office, "Biometric Data-Sharing Process (Five Country Conference (FCC) Data-Sharing Process) Version 7.0" (2016), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/557896/biometric-data-sharing-v7.0.pdf

69 ISO/IEC 19794-4 specifies a data record interchange format for storing, recording, and transmitting the information from one or more finger image. More details available at: https://www.iso.org/standard/50866.html.

70 U.S. Department of Homeland Security, "Privacy Impact Assessment."

71 Ibid.

72 eu-LISA, "Technical Reports on the Functioning of VIS as Per Article 50(3) of the VIS Regulation and Article 17(3) of the VIS Decision" (2018), https://www.eulisa.europa.eu/Publications/Reports/2018%20VIS%20reports.pdf.

73 Bachenheimer, interview.

74 European Commission, "Visa Information System (VIS)," accessed June 5, 2020, https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system_en.

75 e-Estonia, "E-Identity Card," accessed June 5, 2020, https://e-estonia.com/solutions/e-identity/id-card/.

76 e-Estonia, "E-Governance," accessed June 5, 2020, https://e-estonia.com/solutions/e-governance/.

77 e-Estonia, "E-Identity Card."

78 e-Estonia, "Business and Finance," accessed June 5, 2020, https://e-estonia.com/solutions/business-and-finance/.

79 e-Estonia, "What We Learned from the eID Card Security Risk?" accessed July 17, 2019, http://e-estonia.com/card-security-risk/.

80 e-Estonia, "E-Health Record," http://e-estonia.com/solutions/healthcare/e-health-record/.

81 Ibid.

82 European Commission, "Overview of Pre-Notified and Notified eID Schemes Under eIDAS—Estonia," last modified April 2, 2020, https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Estonia.

83 Republic of Estonia e-Residency, "Knowledge Base | Digital ID | Broken, Lost, Destroyed or Stolen," accessed June 5, 2020, https://learn.e-resident.gov.ee/hc/en-us/articles/360000633497-Broken-lost-destroyed-or-stolen

84 e-Estonia, "Interoperability Services—X-Road," accessed June 5, 2020, https://e-estonia.com/solutions/interoperability-services/x-road/.

85 B. Perrigo, "India Has Been Collecting Eye Scans and Fingerprint Records From Every Citizen. Here's What to Know," *Time,* Sept. 28, 2018, https://time.com/5409604/india-aadhaar-supreme-court/.

86 V. Sathe, "The World's Most Ambitious ID Project. Innovations Case Narrative: India's Project Aadhaar," *Innovations* 6, no. 2 (2011), http://www.mitpressjournals.org/doi/pdf/10.1162/INOV_a_00069.

87 Perrigo, "India Has Been Collecting Eye Scans and Fingerprint Records."

88 Ibid.

89 Unique Identification Authority of India, Government of India, "What Is Aadhaar?" accessed June 5, 2020, https://uidai.gov.in/my-aadhaar/about-your-aadhaar.html.

90 Unique Identification Authority of India, Government of India, "Who Is an Introducer?" accessed Oct. 8, 2020, https://www.uidai.gov.in/298-faqs/enrolment-update/enrolment-partners-ecosystem-partners/2027-who-is-an-introducer.html.

91 Unique Identification Authority of India, Government of India, "Biometric Data Capture Guidelines," accessed June 5, 2020, www.uidai.gov.in/298-faqs/enrolment-update/enrolment-partners-ecosystem-partners/2016-what-are-the-uidai-guidelines-for-biometric-data-capture.html.

92 N. Rajan, "Why UIDAI Has Opened Its Eyes to Face Authentication for Aadhaar Card Holders," *The Indian Express,* Jan. 16, 2018, https://indianexpress.com/article/explained/why-uidai-has-opened-its-eyes-to-face-authentication-for-aadhaar-card-holders-5026053/#:~:text=This%20facility%20is%20to%20help,affected%20by%20injury%20or%20disease.&text=The%20UIDAI%20has%20also%20clarified,on%20a%20by%2Dneed%20basis.

93 N. Rajan, "Why UIDAI Has Opened Its Eyes to Face Authentication for Aadhaar Card Holders," *The Indian Express,* accessed July 9, 2019, https://indianexpress.com/article/explained/why-uidai-has-opened-its-eyes-to-face-authentication-for-aadhaar-card-holders-5026053/.

94 International Organization for Standardization, "35.240.15 Identification Cards. Chip Cards. Biometrics: Including Application of Cards for Banking, Trade, Telecommunications, Transport, etc.," accessed June 5, 2020, https://www.iso.org/ics/35.240.15/x/.

95 Unique Identification Authority of India, Government of India, "Enrolment Data Security," accessed June 5, 2020, www.uidai.gov.in/16-english-uk/aapka-aAadhaar/33-enrolment-data-security.html.

96 B.S. Perappadan, "Penalty, Jail Term to Private Entities Storing Aadhaar Data," *The Hindu,* July 4, 2019, https://www.thehindu.com/news/national/penalty-jail-term-to-private-entities-storing-aadhaar-data/article28287174.ece.

97 D. Harwell, "Federal Study Confirms Racial Bias of Many Facial-Recognition Systems, Casts Doubt on Their Expanding Use," *The Washington Post,* Dec. 19, 2019, https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/.

98 Good ID, "Advanced Technologies, Cultural Diversity and Operational Constraints: The Need for Pilots," April 16, 2020, https://www.good-id.org/en/articles/advanced-technologies-cultural-diversity-and-operational-constraints-need-pilots/.

99 Ibid.

100 Fact Check, "Conspiracy Theory Misinterprets Goals of Gates Foundation," April 14, 2020, https://www.factcheck.org/2020/04/conspiracy-theory-misinterprets-goals-of-gates-foundation/.

101 Devex, "The National Team for the Acceleration of Poverty Reduction (TNP2K)," accessed June 5, 2020, https://www.devex.com/organizations/national-team-for-the-acceleration-of-poverty-reduction-tnp2k-indonesia-125277.

102 S.R. Sulaiman, "Govt Readies New Direct Scheme for 'Problematic' LPG Subsidy," *The Jakarta Post,* March 15, 2019, https://www.thejakartapost.com/news/2019/03/14/govt-readies-new-direct-scheme-for-problematic-lpg-subsidy.html.

103 Ibid.

104 CARIN Alliance, "Consumer ID & Authentication," accessed June 5, 2020, https://www.carinalliance.com/our-work/consumer-id-authentication/.

105 Thales Group, "Thales Building Trust in Mobile Apps—The Consumer Perspective" (2020), https://www.gemalto.com/brochures-site/download-site/Documents/tel-consumer-perspectives.pdf.

106 CARIN Alliance, "Consumer ID & Authentication."

107 Federal Communications Commission, "Mapping Broadband Health in America."

108 Good ID, "Advanced Technologies."

109 Sarfraz, "Adermatoglyphia."

110 Grother, Ngan, and Hanaoka, "NISTIR 8280."

111 Harwell, "Federal Study Confirms Racial Bias."

112 K.M. Hoffman et al, "Racial Bias in Pain Assessment and Treatment Recommendations, and False Beliefs About Biological Differences Between Blacks and Whites," *Proceedings of the National Academy of Sciences of the United States of America,* 113, no.16 (2016): 4296–4301, https://doi.org/10.1073/pnas.1516047113.

113 Federal Communications Commission, "Mapping Broadband Health in America."

114 American Health Information Management Association, "Smile, You're on Facial Recognition: Developing Technology Could Solve Patient Identification Issues," accessed June 5, 2020, http://bok.ahima.org/doc?oid=302443#.XuPkwchJFnJ.

115 National Human Genome Research Institute, "Facial Recognition Software Helps Diagnose Rare Genetic Disease," March 23, 2017, https://www.genome.gov/news/news-release/Facial-recognition-software-helps-diagnose-rare-genetic-disease.

116 CARIN Alliance, "Consumer ID & Authentication."

117 International Organization for Standardization, "ISO/IEC 19794-2:2005 Information Technology—Biometric Data Interchange Formats — Part 2: Finger Minutiae Data," accessed June 5, 2020, https://www.iso.org/standard/38746.html.

118 B. Wing, "ANSI/NIST-ITL Standard: Data Format for the Interchange of Fingerprint, Facial, and Other Biometric Information," in *Encyclopedia of Biometrics,* eds. S.Z. Li and A.K. Jain (Boston: Springer, 2015), https://doi.org/10.1007/978-1-4899-7488-4_9045.

119 National Institute of Standards and Technology, "ANSI/NIST-ITL 1-2011 Update: 2015 Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information" (2015), https://www.govinfo.gov/content/pkg/GOVPUB-C13-c740de60818ab51bb0be4f47c343f184/pdf/GOVPUB-C13-c740de60818ab51bb0be4f47c343f184.sp.500-290e3.pdf.

120 The Pew Charitable Trusts, "Patients Want Better Record-Matching."

121 Ibid.

122 N. Jankowicz, "Estonia Already Lives Online—Why Can't the United States?" *The Atlantic,* May 27, 2020, https://www.theatlantic.com/international/archive/2020/05/estonia-america-congress-online-pandemic/612034/.

123 Thales Group, "Biometric Data and Data Protection Regulations (GDPR and CCPA)," last modified May 12, 2020, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/biometric-data

124 M.K. McGinley, K. Brotman, and E.L. Rigney,"The Biometric Bandwagon Rolls On: Biometric Legislation Proposed Across the United States," *The National Law Review,* March 25, 2019, https://www.natlawreview.com/article/biometric-bandwagon-rolls-biometric-legislation-proposed-across-united-states.

Blank page

pewtrusts.org