

CRITICAL COMMENTARY

The Emergence of Biometric Technology in Healthcare: Patient Privacy and Data Protection Concerns

SHALINI GAMBHIR MHA, MRT(T), BSC
APRIL 1, 2021



**JOHNSON
SHOYAMA**

Patient privacy is in grave danger because of new emerging biometric technologies in healthcare organizations primarily driven by the need to improve identification services. This critical commentary argues that the implementation of biometric systems in hospitals will cause the community to be vulnerable to the collection of biometric information without their knowledge and consent. The analysis will also comment on the loss of choice and ultimately control over the collection, disclosure and use of personal data (Office of the Privacy Commissioner of Canada 2011). The challenge is further internalized by unreliable management of privacy information to which it must quickly adapt as technology is advancing rapidly. This paper will also comment on mismatching of identity due to body alteration. To remedy this, healthcare organizations must present a well thought out design and implementation proposal of biometric systems that clearly defines its use and purpose to only improve patient identity without compromising privacy and establish the essential need for health information management leaders and experts in the field of biometrics and healthcare during implementation, system operation and evaluation. Background information on applying biometric systems outside of health care will also be explored to show how its fast trend and convenience globally have immaturely influenced thought leaders in healthcare.

WHAT IS BIOMETRIC TECHNOLOGY?


Biometric technology, an advanced layer of security, collects unique identifiers such as voice recognition, palm and vein scans, facial recognition, and iris and retinal scans by machines and devices (Office of the Privacy Commissioner of Canada 2011). Once the analog information is mapped, the digital data is saved as encrypted data for future access. Kaspersky (2020) details three distinct categories that exist within biometrics: biological, morphological and behavioural. Biological biometrics include genetic or molecular information from DNA or blood samples, morphological biometrics map the body's physical structure such as facial recognition or fingerprints, and behavioural biometrics distinctly identify patterns such as gait, voice cadence and speech.

THE EMERGENCE OF BIOMETRICS INTO SOCIETY

Today, most people are familiar with biometric technology through smartphones and have interacted with facial recognition and fingerprint technology to purchase applications and unlock phones while replacing or augmenting passwords. Other industries include facial recognition with chip technology for electronic passports, fingerprints and iris scans for airports and hospital registration, and NEXUS, a program to help travellers cross the border faster, established the use of iris scans for travellers to confirm their identity. Tragic events, such as 9/11, have resulted in an increase of surveillance cameras with facial recognition capacity in crowded cities to detect possible threats to society using unique algorithms that match with a database of images of potentially dangerous individuals (Dastbaz, Halpan, and Wright 2013).

Kaspersky (2020) researchers state the emergence of biometric technology stemmed as a necessity to reduce identity errors, authenticate individuals who are a possible threat to society, identify and authorize individuals into a restricted zone or personal space and protect private information and data. Today, biometric technology is seen as remarkably convenient and efficient. Identity authentication is quick and the identifiers are part of your body blueprint; you are always identifiable, the biometrics can never be lost and challenging to steal as opposed to a password or a key.

Technology journalist Murgia (2019) passionately details in her Ted Talk that every time an individual interacts with the connected world, whether through a phone application, surveillance camera, or website, biometric technology is designed to log every behavioural attribute, daily habit and movement, essentially one's life converted into a data package. This tracking reveals unpredicted things about an individual's belief pattern, likes and dislikes, cultural values, conviction of felonies, and diagnosed health problems. Murgia (2019) continues that the biological data collected by biometrics "identifies you for life" and the "body is the new currency in the data market," and if misused or lost, can result in irreversible damage. An article by Digital Synopsis (2020) describes how Ogilvy and Mather, an Ad agency, partnered with "Hong Kong Cleanup Challenge" to release a city-wide social change campaign entitled "The



Face of Litter". Forensic DNA analysis of the trash samples predicted and generated facial reconstruction of the litterers. The portraits of these litterers were then posted around the city to support the campaign. A vivid cue of how your personal life and habits can unexpectedly be interfered with and revealed by your DNA blueprint.

PRIVACY AND DATA PROTECTION CHALLENGES IN HEALTHCARE

Biometric technology has captured the attention and excitement of healthcare leaders, scientists, and engineers in the medical industry resulting in these systems to slowly attempt integration and find a functional use in healthcare patient safety. Researchers Sohn et al. (2020, 1) developed a Biometric Automated Patient and Procedure Identification System (BAPPIS) to reduce patient authentication mistakes that lead to medical errors in radiotherapy and surgery departments. The verification system introduced a two fingerprint patient authentication process along with other identifiers such as a photograph and date of birth at the time of registration. The new system was studied across 143 patients and concluded there were no false-positive errors and that 96.9% of the time fingerprints were correctly identified when electronic health records and patient plans were recalled and matched (Sohn et al. 2020, 7-8). An interesting international study in Western Kenya by Sight, Kitayimbwa, and Were (2020) discussed the challenges of unique reliable patient identifiers in developing countries with limited resources. The researchers found that an open-source facial recognition technology system performed with a 99% sensitivity rate as it identified almost all patients when matched. The false acceptance rate was less than 1%.

In contrast, Nigam et al. (2019) found that patients with cataract surgeries altered the texture pattern of the iris, confusing previously saved iris scans. The scientists uncovered that the iris scans were only 25% accurate after surgery. Similarly, scientists Bouguila and Khohtali (2020) analyzed literature from 2000 - 2019 and reviewed the discrepancy with facial recognition technology after facial plastic surgery. It was found that there was a significant alteration to the face which resulted in challenging matches with facial algorithms. This is of

great concern in the medical industry as patient mismatches can result in privacy breaches amongst patients and cause medical errors. Finger amputations have seen similar challenges with fingerprints. An interesting theme continues to emerge in the field of biometrics that is of full and informed consent. Are patients aware of the interaction between their new facial features and old facial algorithms prior to the surgery? Do they have the knowledge to advocate for themselves in case of an identity error post-facial surgery? Researchers Bouguila and Khohtali (2020) continue the discussion by encouraging plastic surgeons to be prepared to have conversations around biometric technology, privacy concerns, and authentication errors. There is currently a disconnection between biometric technology intelligence and body alteration. It is important to note that altering biometrics unnaturally will confuse the technology, however, most machines are designed to understand natural ageing and changes in texture and skin. This paradigm shift in technology is predestined to infiltrate into clinical environments, however, time is needed for the technology to fine-tune before introducing it to the medical industry.

Studies that show promising biometric systems in healthcare are fairly new and one must not be naive to believe that healthcare organizations have invested in sophisticated health information management systems seasoned with biometric experts to protect the personal privacy of patients. Although biometrics has existed in other industries for years and has had an opportunity to design refined privacy systems, it is fairly new to the medical industry. Lawyers and thought leaders Backman and Baer (2019) caution that the federal Privacy Act may have guidelines in place for storing biometric images and data, however surveillance of biometric characteristics is not captured in the act. Regulation of biometric data is still in its infancy stages and the Office of the Privacy Commissioner of Canada (2020) is currently updating its biometric use guidelines and law enforcement. It is safe to say that the medical industry would be taking a critical risk by adopting technology without being legally accountable and responsible for their citizens' privacy.

With the rapid widespread adoption of cloud computing, cybersecurity threats and skilled hackers are on the rise. Researchers at Kaspersky (2019) predict as technology

advances and evolves in ways that are unimaginable and at a fast speed that healthcare organizations most naturally cannot keep up, cyber-attacks will increase without proper privacy infrastructure. These systems are complex, and great attention is required for their oversight. In recent news, Ontario hospitals were attacked by malicious malware, electronic medical records in Saskatchewan were compromised and the Nova Scotia Health Authority experienced a cyber attack that leaked details of patient surgeries (Burke 2020). It is often the case that healthcare organizations immaturely adopt new technologies without being fully prepared, possibly to keep up with the evolution of the economy and a profitable revenue stream. Governments have a responsibility to ensure healthcare funding is dedicated to hospitals, physicians, drugs and clinical care, all other departments, especially Information Technology, end up with minimum funding, unfortunately. There is of course a certain level of risk any industry must accept as technology advances, however with the continued overwhelm of breaches it is vital for the medical industry to revamp their privacy policies and invest in quality health information management professionals, experts in interoperability, health informatics and cybersecurity. Adopting biometrics would only overwhelm and overburden these departments without the financial and strategic support it requires.

The opportunity to provide personal information voluntarily and be informed of how personal data may be used is a basic human right and entrenched in the Federal Privacy Act and provincial privacy laws. Consent is a personal choice where one can dictate what personal information is to be shared, a sense of control exists. A relatable quote from Clarke (2006) states that privacy is an individual's integrity, where 'personal space' is desired without intrusion from others. Biometric data can collect information covertly such as facial recognition by surveillance cameras in patient waiting rooms and fingerprint scan maps by sensors on hospital doors. Meaningful and informed consent should provide a wholesome picture of what data will be collected, why it is collected and the purpose of disclosing, storing and using data in the future and perhaps information on risk management. This is important for patients to feel in control of their identity and not simply give it away for free (Boeckhout, Zielhuis and Bredenoord 2018). In a

legal case of interest, a healthcare worker at Rouge Valley Hospital in Ontario disclosed and sold personal information of 8,300 maternity patients to Global RESP Corporation where the intent of the company was to sell a Registered Education Savings Plan to the newborn children. This was considered a major privacy breach where Global did not obtain consent to access private information from the patients and the healthcare worker breached privacy by unauthorized access and disclosure of private information to a third party (CanLII 2015, 108273). This is a prime example of foreshadowing the potential risk of wrongful disclosure or misuse of biometric data without consent such as genetic information and a history of chronic illness which could be very valuable to health insurance companies dictating the fate of opting into insurance or high premiums. The danger of biometric data is that it not only contains genetic, morphological and behavioural data, but secondary data such as culture, religion, and occupation. Experts Backman and Baer (2019) caution if this secondary information is necessary for health care and also if patients are aware of this in-depth disclosure of their life and the potential ramifications if leaked. Cross-matching is another privacy risk. Patients tend to provide biometric data for one database, however with cross-matching technology this data can be used in multiple other databases without consent. Sadhya and Singh (2017) found cross-matching of biometric data to increase the risk of privacy, suggesting that patients must take vigilance and be attentive to this irreplaceable data. The researchers investigated linking databases to decrease the privacy risk, but were unsuccessful.

It is clear that consent is vague and covert when interacting with biometric systems, not in compliance with the Privacy Act and coupled with high-security breaches. Nonetheless, the gradual presence of biometric systems in healthcare organizations is inevitable. The potential role of blockchain technology paired with biometric systems is promising in maintaining the privacy and confidentiality of patients and can enhance interoperability standards as discovered in a medical informatics study by Abu-elezz et al. (2020). First introduced through Bitcoin cryptocurrency technology in 2008 by Satoshi Nakamoto, blockchain in healthcare settings have the potential to protect healthcare data and identity management specifically connected with patient

consent and autonomy with blockchain automation and warrants further exploration (Abu-elezz et al. 2020).

ALTERNATIVES AND NECESSITY

All the literature in this analysis that shows the promising value of biometric technology in the medical industry failed to compare their results with other multiple-factor authentication systems to show the necessity of biometric technology. For example, commonly in radiation oncology, a four-factor multiple authentication system is used. This includes the patient's date of birth, full name, photo identification and the treatment plan identification name. There has been great success with this identification system as it helps solve the problem of correctly identifying a patient and matching them to their correct patient record. Thus, one may reconsider the necessity to implement a biometric system along with its privacy nuances if another simplified and adequate solution exists. Would a biometric system ethically sit well with a patient and be in line with their values of quality health care?

CONCLUSION

Although benefits of biometric technology in healthcare may be affordable and scalable and may help correctly authenticate a patient faster, reduce costs in medical errors and correct for duplicate medical electronic charts, provide convenience and speed and a rather unique excitement for patients as they interact with new technology, the risks and challenges outweigh the benefits without responsible execution. Biometric technology remains in its infancy where nuances such as surgical body changes and its interaction with biometric systems must still be refined. Healthcare information management and privacy do not have the expertise nor the funding for a supportive foundation to securely manage and protect patient's health information as elite companies like Apple Inc. An unfortunate gap in the system is the lack of standardization, regulation and law enforcement of biometric data and images which gives rise to challenges in authenticating patients, enforcing policies, medical errors, and opportunities for litigation. Despite these challenges, biometric adoption can be supported by greater regulation, policy development, and by engaging and strengthening the health care

system to build greater capacity to respond to the privacy and security threats this innovation is challenged with. A common theme of covert consent and biometric technology and loss of choice and control seem to stretch across the literature, however, the introduction of blockchain technology may help alleviate this strain. The strategic goals and vision of the healthcare organization must ultimately align with the emergence and purpose of innovative biometric technology, and with accountable and responsible safety platforms the technology is welcomed.

ABOUT THE AUTHOR

Shalini is uniquely trained in cancer radiotherapy and has established herself as a technical expert in cancer management. Having witnessed the modernization of cutting-edge technology and groundbreaking inventions, Shalini has been fortunate to function as a frontline therapist, challenged daily to adapt to a complex and unpredictable healthcare system, questioning the status quo by aligning herself to quality patient care. With over a decade of experience, she can also be credited for her contribution to developing and launching the first Head and Neck Cancer Support Program in Vancouver in 2019. Shalini holds a Master of Health Administration degree from the University of Regina and currently resides in Vancouver, BC. She is particularly passionate about Health Information Management and the integrative risk assessment between patient safety, privacy and security and has plans to be impactful in policy capacity and grassroots advocacy for vulnerable patients. In addition to her primary job functions, Shalini has been recognized for her volunteer contributions to poverty alleviation, education, anti-violence, and food security in her community and during her international volunteer trip to Nepal, Pokhara.



REFERENCES

- Abu-elezz, Israa, Asma Hassan, Anjanarani Nazeemudeen, Mowafa Househ and Alaa Abd-alrazaq. 2020. "The benefits and threats of blockchain technology in healthcare: A scoping review." *International Journal of Medical Informatics* 142: 1-9.
- Ampamya, Sight, John Kitayimbwa, and Martin Were. 2020. "Performance of an open source facial recognition system for unique patient matching in a resource-limited setting." *International Journal of Medical Informatics*. (141).
- Backman, Paige and Aaron Baer. 2019. "Canada: Biometric identification and privacy concerns. A Canadian perspective." *Mondaq*. Accessed January 21, 2021. <https://www.mondaq.com/canada/privacy-protection/808754/biometric-identification-and-privacy-concerns-a-canadian-perspective>
- Boeckhout, Martin, Gerhard A. Zielhuis, and Anneien L. Bredenoord. 2018. "The FAIR guiding principles for data stewardship: fair enough?" *European journal of human genetics* 26 (7): 931–936.
- Bouguila, J., H. Khochali. 2020. "Facial plastic surgery and face recognition algorithms: Interaction and challenges. A scoping review and future directions." *Journal of Stomatology, Oral and Maxillofacial Surgery* 121 (6): 696-703.
- Burke, David. 2020. Hospitals 'overwhelmed' by cyberattacks fuelled by booming black market. Accessed January 23, 2021. <https://www.cbc.ca/news/canada/nova-scotia/hospitals-health-care-cybersecurity-federal-government-funding-1.5493422>
- Clarke, Roger. 2006. "What's 'privacy'?" *Roger Clarke's Website. Xamax Consultancy Pty Ltd*. Accessed January 25, 2021. <http://www.rogerclarke.com/DV/Privacy.html>
- Dastbaz, Mohammad, Edward Halpan, and Steve Wright. 2013. "Emerging technologies and the human rights challenge of rapidly expanding state surveillance capacities." *Strategic Intelligence Management*, edited by B. Akhgar and S. Yates, 108-118. United Kingdom: Butterworth Heinemann.
- Digital Synopsis. 2020. "Anti-litter campaign from Ogilvy HK uses DNA to identify offenders and shame them." Accessed March 1, 2021. <https://digitalsynopsis.com/advertising/the-face-of-litter-ogilvy-mather-hong-kong/>
- Global RESP Corporation accountable for actions of sales representative for the use of patients' personal information purchased from a Rouge Valley Hospital employee, 2015 CanLII 108273 (PCC), <<https://canlii.ca/t/h3p59>>, retrieved on 2021-01-31
- Kaspersky. 2020. *What is biometrics security?* Accessed January 14, 2021. <https://www.kaspersky.com/resource-center/definitions/biometrics>
- Kaspersky. 2019. *4 Cyber security trends to keep an eye on*. Accessed January 14, 2021. <https://www.kaspersky.com/resource-center/preemptive-safety/cyber-security-trends>
- Murgia, Madhumita. 2019. "The business of biometrics." *TEDxGateway*. Accessed January 14, 2021. https://www.youtube.com/watch?v=w2l8HlhDy_s
- Nigam, Ishan, Rohit Keshari, Mayank Vatsa, Richa Singh, and Kevin Bowyer. 2019. "Phacoemulsification cataract surgery affects the discriminative capacity of iris pattern recognition." *Scientific Reports* 9: 11139.
- Office of the Privacy Commissioner of Canada. 2011. *Data at your fingertips biometrics and the challenges to privacy*. Accessed January 3, 2021. https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/gd_bio_201102/

Sadhya, Debanjan and Sanjay Kumar Singh. 2017. "Privacy risks ensuing from cross-matching among databases: A case study for soft biometrics." *Elsevier* 128: 38-45.

Sohn, Jason, Haksoo Kim, Samuel Park, Soyoung Lee, James Monroe, Thomas Malone, Timothy Kinsella, Min Yao, Charles Kunos, Simon Lo, Robert Shenk, and Mitchell Machtay. 2020. "Clinical study of using biometrics to identify patient and procedure." *Frontiers in Oncology* 10: 1-9.