Does deidentification of data from wearable devices give us a false sense of security? A systematic review

Lucy Chikwetu, Yu Miao, Melat K Woldetensae, Diarra Bell, Daniel M Goldenholz, Jessilyn Dunn**

Wearable devices have made it easier to generate and share data collected on individuals. This systematic review seeks to investigate whether deidentifying data from wearable devices is sufficient to protect the privacy of individuals in datasets. We searched Web of Science, IEEE Xplore Digital Library, PubMed, Scopus, and the ACM Digital Library on Dec 6, 2021 (PROSPERO registration number CRD42022312922). We also performed manual searches in journals of interest until April 12, 2022. Although our search strategy had no language restrictions, all retrieved studies were in English. We included studies showing reidentification, identification, or authentication with data from wearable devices. Our search retrieved 17 625 studies, and 72 studies met our inclusion criteria. We designed a custom assessment tool for study quality and risk of bias assessments. 64 studies were classified as high quality and eight as moderate quality, and we did not detect any bias in any of the included studies. Correct identification rates were typically 86–100%, indicating a high risk of reidentification. Additionally, as little as 1–300 s of recording were required to enable reidentification from sensors that are generally not thought to generate identifiable information, such as electrocardiograms. These findings call for concerted efforts to rethink methods for data sharing to promote advances in research innovation while preventing the loss of individual privacy.

Lancet Digit Health 2023; 5: e239–47

Published **Online** February 14, 2023
https://doi.org/10.1016/S2589-7500(22)00234-5

*Contributed equally

Department of Electrical and Computer Engineering (L Chikwetu MSc) **and Department of Biomedical Engineering** (Y Miao BSc, M K Woldetensae, D Bell BA, J Dunn PhD), **Duke University, Durham, NC, USA; Department of Neurology, Beth Israel Deaconess Medical Center, Boston, MA, USA** (D M Goldenholz MD); **Department of Neurology, Harvard Medical School, Boston, MA, USA** (D M Goldenholz)

Correspondence to:
Dr Jessilyn Dunn, Department of Biomedical Engineering, Duke University, Durham, NC 27708, USA
jessilyn.dunn@duke.edu

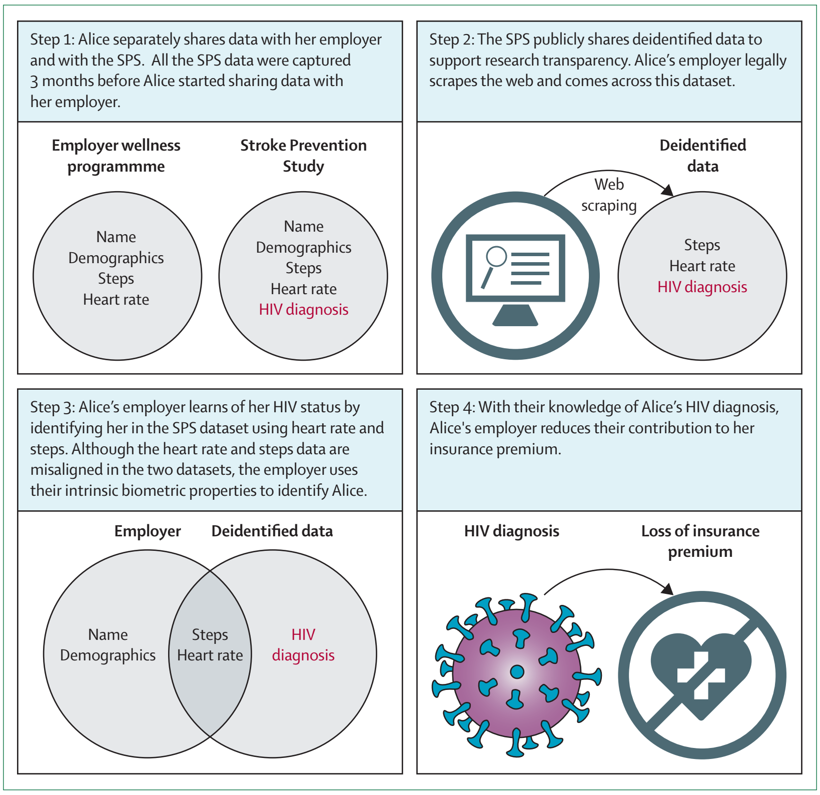
Introduction

The wearable device market, worth US$116·3 billion in 2021, is projected to be worth $265·4 billion by 2026.[1] These wearable devices often include digital health technologies such as consumer smartwatches that monitor an individual's heart rate (with photoplethysmography technology) and step count (with accelerometry), and other body-worn sensors—eg, those that continuously monitor blood glucose concentration. Digital health technologies are becoming increasingly diverse in their body location, sensor array, and capabilities. Some wearable devices have proven medical applications—eg, for detecting arrhythmias[2] or infections.[3] Generally, data from wearable devices are persistent[4] and have the potential to be shared widely to improve the accuracy and generalisability of algorithms. To support advancements in research that improves human health (eg, through secondary data analysis), the US National Institutes of Health has adopted policies encouraging extensive data-sharing practices, starting in 2023. Additionally, many institutions are adopting the Findable, Accessible, Interoperable, and Reusable (FAIR) Guiding Principles for scientific data management and stewardship.[5] Although data sharing provides tremendous benefits, it also poses many crucial questions around privacy risks to patients and study participants that remain unanswered. For example, could machine-learning algorithms be applied to public datasets or data shared through third-party data-sharing agreements to enable reidentification? Is there an opportunity for data misuse by governments, corporations, or individuals? If so, how significant is this risk, and is there a way to mitigate it?

In this systematic review, we define reidentification as the act of determining an individual's identity from deliberately deidentified or anonymised data. Reidentification often involves relinking a deidentified or anonymised dataset with a dataset that has identifiers to establish users present in both. Merely matching data does not constitute reidentification. Instead, there is a need for identifiers for reidentification to take place. In real-world scenarios, identifiers are not always available; however, unethical individuals or organisations who want to know more about individuals whose data they already possess might have them (figure 1). In addition, data breaches[6] can also lead some individuals or organisations to possess a complete list or subset of identifiers. For this systematic review, we assume motivated individuals or organisations gain access to identifiers and build machine-learning algorithms to relink or match biometric signals.

As a result of reidentification, the release of seemingly innocuous data can have unforeseen consequences. One notable example is the reidentification of the Massachusetts Governor from publicly shared and seemingly deidentified state employee health insurance data,[7,8] which led to the passing of the Health Insurance Portability and Accountability Act in 1996.[9] This example also shows that regulation changes often lag behind real-world reidentification events and their consequences. With biomedical data, the consequences of reidentification could be dire (eg, figure 1). Advances in machine learning have made it possible to infer sensitive information about individuals, such as their medical diagnoses,[10] mental health,[11] personality traits,[12] and emotions,[13] thus making it possible to learn information that an individual has not directly shared. Reidentification, therefore, can reveal not only the initially collected data but also such inferences about an individual. As more people acquire knowledge about the risk of reidentification, we are seeing a growing body of literature from various sources, including researchers simulating reidentification attacks[14,15] and governments informing their citizens about the risks of reidentification.[16]

For more on the **data sharing practices from the US National Institutes of Health** see https://sharing.nih.gov/



Step 1: Alice separately shares data with her employer and with the SPS. All the SPS data were captured 3 months before Alice started sharing data with her employer.

Step 2: The SPS publicly shares deidentified data to support research transparency. Alice's employer legally scrapes the web and comes across this dataset.

Step 3: Alice's employer learns of her HIV status by identifying her in the SPS dataset using heart rate and steps. Although the heart rate and steps data are misaligned in the two datasets, the employer uses their intrinsic biometric properties to identify Alice.

Step 4: With their knowledge of Alice's HIV diagnosis, Alice's employer reduces their contribution to her insurance premium.

Figure 1: **An example scenario with an employee with HIV who does not wish to share their HIV status with their employer but this information is divulged unintentionally through data sharing with the Stroke Prevention Study**
SPS=Stroke Prevention Study.

For more on the **Covidence software** see https://www.covidence.org/

See Online for appendix

Fundamentally, data from any sensing modality that can create a unique digital identifier (ie, a so-called fingerprint) can potentially be used for biometric identification or authentication (eg, iris scans, face scans, and voice prints). Any such data can be used to reidentify an individual.[15]

This paper explores open questions surrounding reidentification through an extensive systematic review of available literature. For example, what types of data from wearable devices, how much of that data, and what resolution of such data can enable reidentification are all crucial questions that remain unanswered. Our goal is to provide an overview of reidentification risks from wearable devices that are often not considered as generating identifiable information.

Methods

This systematic review follows PRISMA guidelines[17] and is registered on PROSPERO (CRD42022312922).

Information sources

We searched peer-reviewed literature indexed on Web of Science, IEEE Xplore Digital Library, PubMed, Scopus, and the ACM Digital Library on Dec 6, 2021, with no start date restrictions. We also searched journals that deal with biometric technologies (eg, P*attern Recognition Letters* and *IEEE Sensors*). In April 2022, we identified a newly published review article[18] in a journal we were monitoring that explores some of the topics discussed here; however, our systematic review employed a broader search strategy, found additional sensing modalities, and delved deeper into reidentification. Additionally, our systematic review focuses on the biomedical research community, which is newly charged with public data requirements. We used Covidence software to conduct this review.

Search strategy

This systematic review focused on the reidentification of individuals from biometric signals from wearable devices, as opposed to other forms of reidentification, such as camera-based reidentification. We excluded GPS-based technologies or biometrics widely used for identification (eg, iris scans and fingerprints), as these present clear privacy risks.[19] Although we primarily focused on studies conducted using common wearable devices, to highlight what could be possible we also report findings from currently uncommon wearable devices, such as the seismocardiogram and the phonocardiogram, even if the measurement modality was not a wearable form factor. The keywords we used for our searches were "re-id* OR reid* OR identi*" and "biometric* OR biosensor*" together with various words identifying sensors such as "acceleromet*", "gyroscope", "ECG", "PPG", and "phonocardiogra*" (the full search strategy is available in the appendix pp 2–5). Given search functionality restrictions in IEEE Xplore, we decomposed the IEEE Xplore database search into multiple separate searches that met the required guidelines. Our search strategy did not restrict the language in which articles were published; however, all retrieved studies were in English.

Eligibility criteria

All included studies were peer-reviewed journal and conference papers published before April 12, 2022. We considered experimental studies, systematic reviews, meta-analyses, and cohort studies. Eligible studies had to show reidentification, identification, or authentication using biometric signals collected in humans using wearable devices except in circumstances of rare sensors such as the phonocardiogram, which could include biometric monitoring technologies with non-wearable form factors. Additionally, we only included studies with unimodal sensors, since we did not come across any studies where unimodal sensors failed to perform reidentification when used independently yet succeeded when combined with other sensors.

We excluded studies that used animals, used theoretical models, used video or cameras, employed impractical form factors (such as multiple inertial measurement unit [IMU] sensors attached to five locations[20]), did not describe sensor placement, had unclear sensor specifications, or did not report standard performance metrics. We also excluded 28 studies with similar findings to other studies by the same authors. To avoid duplicate studies when dealing with systematic reviews and meta-analyses, we only included studies in the reviews or analyses that were not yet appearing on our list of included studies and excluded the systematic review or meta-analysis itself.

Screening and selection

We exported all studies to Covidence, which automatically identified and removed 6218 duplicates. Two independent reviewers performed title and abstract screening (LC and YM) and full-text review (LC and DB), and a third reviewer acted as the adjudicator (DB for title and abstract screening and YM for full-text review) resolving inter-rater disagreements. LC ensured quality assurance of the process, and all reviewers resolved any resulting anomalies after adjudication.

Data extraction and synthesis

Two reviewers (LC and YM) independently extracted data and performed study quality and publication bias assessments for each study and an adjudicator (MKW) resolved all conflicts. If any included study had tables that referenced other studies, we performed a nested search to check if any of these studies met our eligibility criteria, and if so extracted information from those studies. We extracted 18 study characteristics from the included studies (appendix pp 5–6) and sensing-modality-specific characteristics—the number of channels or leads (electrocardiogram [ECG], electroencephalogram [EEG], and electromyogram) and the evoked potential stimulus (EEG).

To minimise error, LC reviewed the extracted data for potential discrepancies and all team members resolved any identified issues. All graphs were generated in R (v4.0.2) with ggplot2.

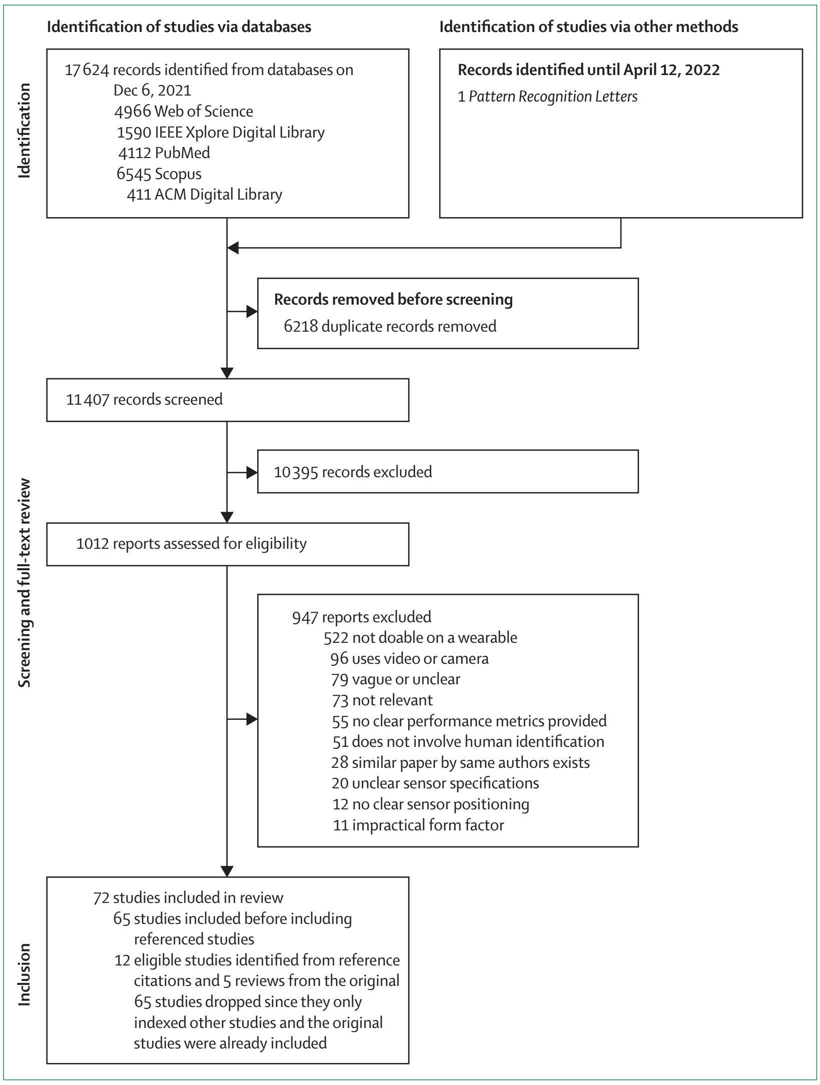

Identification of studies via databases
Identification of studies via other methods
Identification
17 624 records identified from databases on Dec 6, 2021
4966 Web of Science
1590 IEEE Xplore Digital Library
4112 PubMed
6545 Scopus
411 ACM Digital Library
Records identified until April 12, 2022
1 *Pattern Recognition Letters*
Records removed before screening
6218 duplicate records removed
Screening and full-text review
11 407 records screened
10 395 records excluded
1012 reports assessed for eligibility
947 reports excluded
522 not doable on a wearable
96 uses video or camera
79 vague or unclear
73 not relevant
55 no clear performance metrics provided
51 does not involve human identification
28 similar paper by same authors exists
20 unclear sensor specifications
12 no clear sensor positioning
11 impractical form factor
Inclusion
72 studies included in review
65 studies included before including referenced studies
12 eligible studies identified from reference citations and 5 reviews from the original 65 studies dropped since they only indexed other studies and the original studies were already included

Figure 2: PRISMA diagram illustrating the study selection process

Results

Our search retrieved 17 625 studies (which included 6218 duplicates), resulting in 11 407 studies to be screened (figure 2). After title and abstract screening, 1012 studies advanced to the full-text review. Of these, 65 met the eligibility criteria. Through a nested search of the tables in the 65 studies we uncovered an additional 12 studies. We also removed five studies from the original 65 since they were review articles that referenced other studies we had included. Finally, we extracted data from included studies and subsequently analysed them (appendix pp 6–12). We were left with 72 non-repeated, eligible studies.

For assessment of study quality, standard clinical study assessment tools[21] were not applicable because none of the included studies were clinical. Instead, we designed a custom assessment tool with four overall quality categories: high, moderate, low, and very low (appendix p 13). Of the 72 reviewed studies, 64 (89%) were classified as high quality, eight (11%) were moderate quality, and none were low quality. We detected no publication bias[22] in any of the included studies through our custom tool for study quality analyses and risk of biases (appendix pp 14–18).

In the included studies, 20 unique sensing modalities were mentioned (figure 3), the top three of which were EEG (n=17), IMU (n=15), and ECG (n=8). Despite the abundance of photoplethysmogram-enabled smartwatches,[23] our search revealed less investigations on photoplethysmography (n=4) than on ECG (n=8), and our complete set of retrieved studies (ie, before selection and screening) revealed the same pattern, with 297 papers on photoplethysmography and 775 on ECG in the initial, unscreened search. Furthermore, in addition to studies using common sensing modalities, there were a few studies using less common biosignals such as seismocardiogram and bioimpedance, indicating the importance

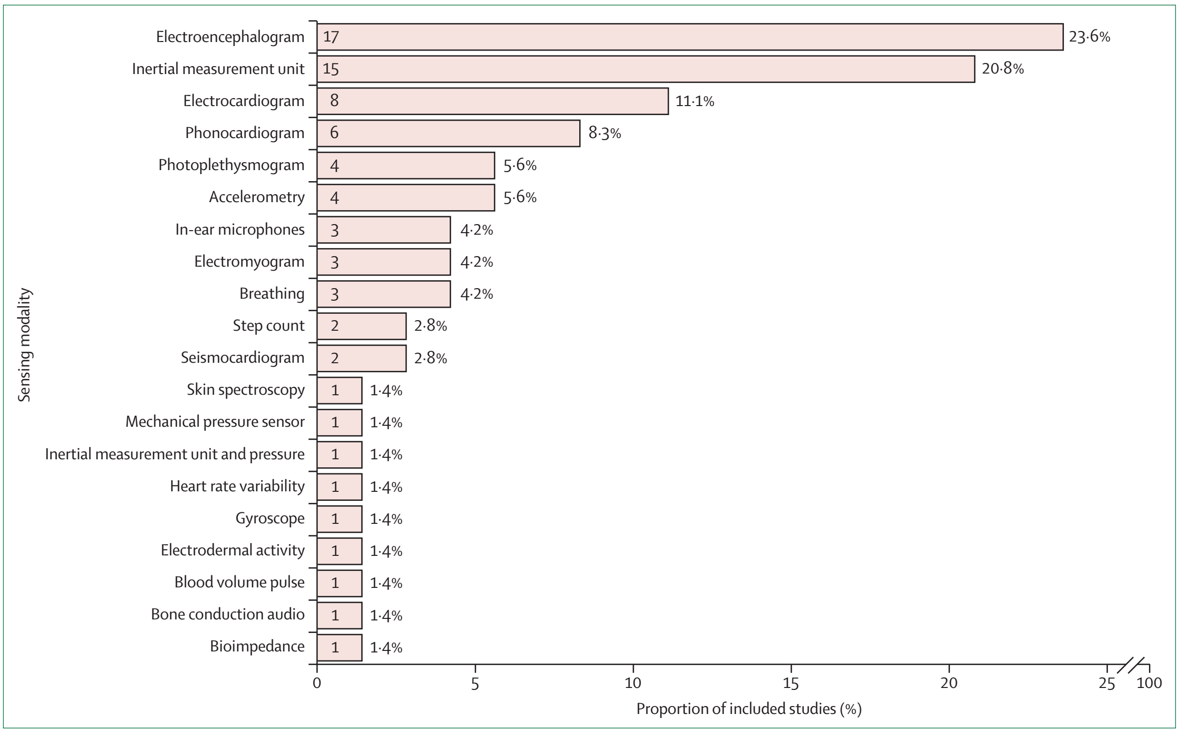


***Figure 3:* Frequency of appearance of sensing modalities in explored studies**

Frequency (number inside bars) is the count of sensing modalities that are examined in the 72 studies explored, and the percentage is the proportion of papers covering that sensing modality. Some papers explored more than one sensing modality; hence the number of all sensing modalities (76) is more than the number of papers explored (72). Here, inertial measurement unit involves the simultaneous use of an accelerometer and gyroscope, and does not include a magnetometer.

of privacy considerations even in emerging sensing technologies.

Not all 18 study characteristics were present in every paper (appendix p 1); however, every included study reported biometric identification performance (how well the system performed on the task of identifying individuals), which was our key variable of interest. Because 57 (79%) of the papers used correct identification rate (CIR) as the biometric performance metric, we focus our findings on CIR; however, there are other widely accepted biometric performance metrics, such as the equal error rate, which was reported by 22 (31%) of the included studies. Notably, of the 25 studies that reported participants' health status, all but one participant[24] was reported to be healthy. This participant had a heart condition that reportedly made their identification easier.[24]

We analysed the body positioning of all wearable devices used (figure 4). The majority of the devices were positioned on the wrist (26), head (16), or chest (13), and some of the sensing modalities were tested on multiple body locations (eg, ECG was measured using sensors behind the ear, on the upper arm, on the chest, or on the wrist). In addition, two studies explored how wearable device placement affects reidentification. Noh and colleagues[25] found that the bioimpedance CIR was higher at the wrist (95·7%) than at the finger (77·6%), and Zhang and colleagues[26] found the ECG CIR to be higher using measurements from a single arm (98·8%) than using electrodes next to each ear (91·1%).

We explored the biometric identification performance of the studies with the highest number of participants for each sensing modality (appendix p 2) and high CIRs were observed, ranging from 87% (keystroke dynamics; n=49) to 100% (seismocardiogram; n=20). We also explored the minimum data needed for reidentification (figure 5). Unfortunately, 51% of the studies did not report this characteristic; however, those that did revealed that little data are required. For example, as little as 30 s of typing data (accelerometer and gyroscope data from an Android Wear smartwatch; Google, Mountain View, CA, USA) could achieve a CIR of 99·2% for a 34-person participant pool.[27]

Given that EEG, IMU, and ECG had the largest bodies of evidence on reidentification potential, we summarised findings from these three sensor modalities. Although reidentification using IMUs has been explored when individuals perform activities of daily living (eg, eating,[28] brushing one's teeth,[28] or typing[27,29]), over 50% of the studies that used IMUs focused on gait. Accordingly, we elaborate on gait later, and the appendix (p 10) provides tables of study characteristics of other included studies using IMUs that focused on aspects of movement other than gait. IMU sensors, which typically include a triaxial accelerometer and gyroscope, are often incorporated into common consumer products such as smartwatches and smart rings. These sensors are useful not only for activity recognition, but also for fall detection and seizure detection.

EEG

17 studies showed an ability to identify an individual using EEG (average group size 20; median 16; range 4–60; appendix pp 7–8). Five (29%) of these studies reported the recording length used for reidentification, which was 21 s on average, with a median of 12·8 s. 11 (65%) of the studies reported the health status of participants (all were healthy and aged 18–40 years). Activities during signal acquisition included listening to one's favourite music, resting with eyes open or closed, cognitive loading tasks, imagined speech, and visual stimuli. The highest recorded CIR was 99·46% using a four-channel Muse EEG headset (Muse, Toronto, ON, Canada) while participants (n=20) listened to their favourite songs.[30] The system that could enable reidentification with the least amount of data was the MindWave Mobile (NeuroSky, San Jose, CA, USA), a single-channel EEG, that was used during rest with eyes open (n=46) and achieved a CIR of 95·48% with just 2 s of recorded data.[26]

ECG

Eight studies showed an ability to identify an individual using only an ECG signal (average group size 15; median 10; range 5–33; appendix pp 6–7). Three (38%) of the studies reported the health status of participants. All participants were healthy except for a man with cardiopathy aged 60 years in the Randazzo and colleagues study,[24] which used a custom ECG watch (with 1 lead, 1 kHz) to monitor six participants over an unspecified period, during which time they captured 20–63 ECGs per participant. The overall CIR of the study was 99%, and the 60-year-old man with cardiopathy was reported to be the easiest to identify (CIR=100%). A separate study with the VitalJacket (1 lead, 200 Hz; Biodevices, Setúbal, Portugal) attained nearly 100% CIR for five healthy firefighters with single heartbeats that were collected between 5 hours and 6 months after the training data.[31] Even with 6 months between training and testing data, the proposed system could still identify all five firefighters with 100% or near-100% CIR. Finally, the most extensive study (n=33; all healthy)[32] used 1-lead apparel (OMsignal, Montreal, QC, Canada) over 6 weeks in free-living conditions; with just ten heartbeats, the study team's algorithm could identify an individual with a CIR of 95·95%.

Gait

We define gait as an individual's way of walking. 13 studies showed an ability to identify an individual using only gait signals (average group size 34; median 30; range 8–60; appendix pp 9–10). However, only one of the studies reported the health status of its participants, who were all healthy.[33] 12 studies combined the accelerometer and gyroscope, which we refer to as an IMU, or used each sensor independently. Additionally, one study used an in-ear microphone to measure gait from walking sounds propagated through the human musculoskeletal system.[34] One of the challenges in gait studies was the presence of multiple definitions of movement (eg, fixed time durations, step cycles, and walk cycles), thus making it difficult to compare results across studies. However, in one study of note (n=30),[35] just 10 s of data from an IMU (100 Hz accelerometer and gyroscope), the MetaWear C Board wristband (San Francisco, CA, USA), was sufficient to identify an individual with 100% CIR.

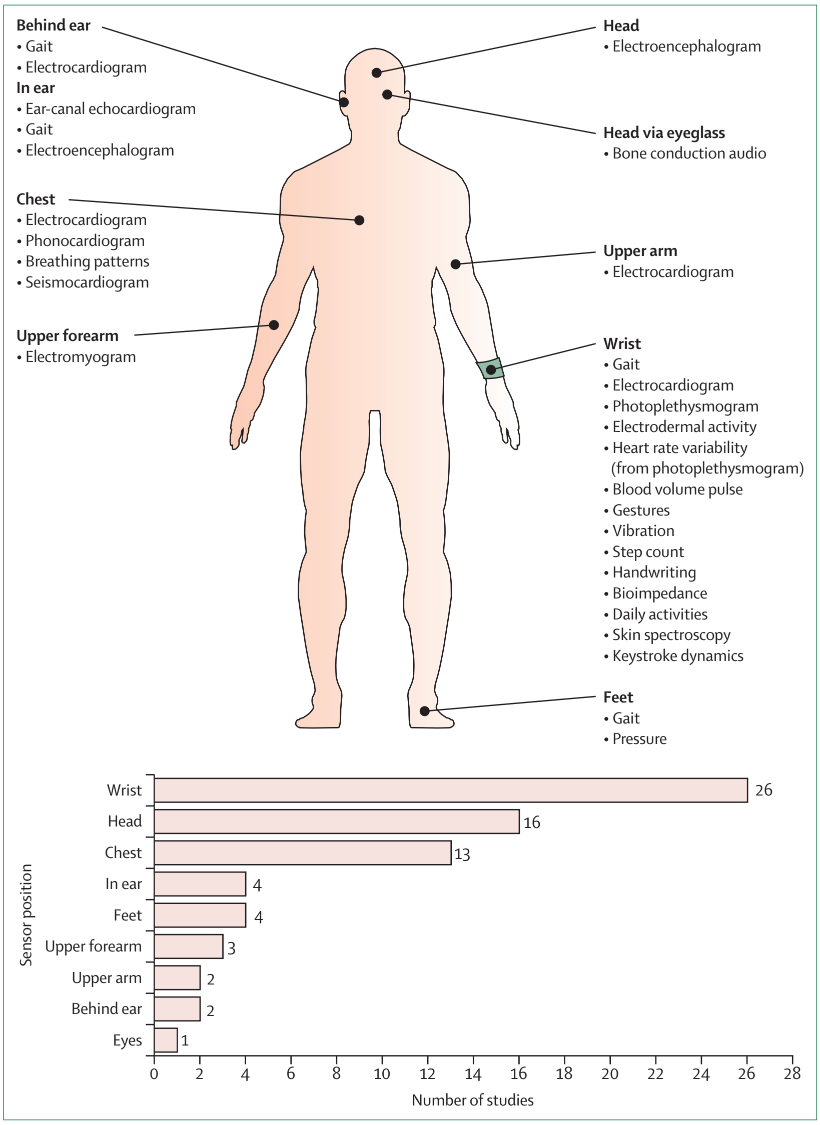


Figure 4: **Sensor positions for the included studies**
This illustration excludes two studies that performed biometric identification using breathing sounds from a smartphone held in participants' hands.

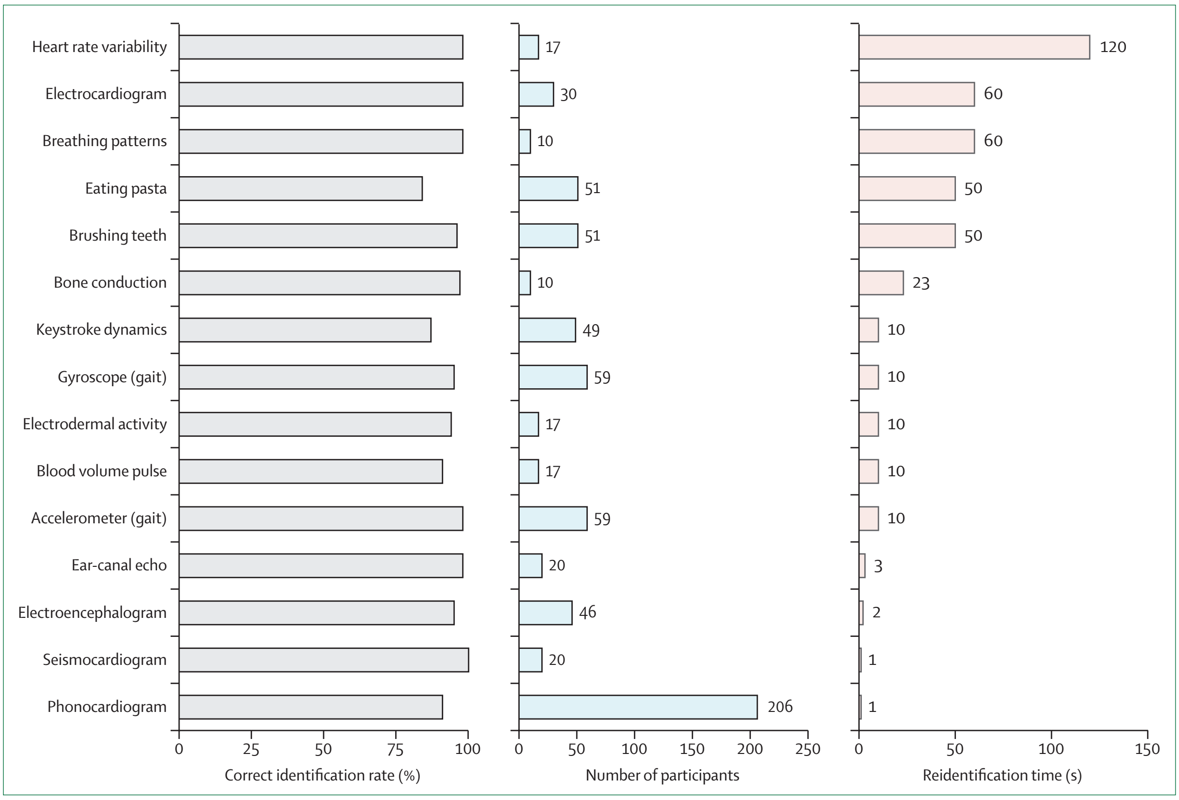


***Figure 5*: Correct identification rate, number of participants, and the minimum amount of time needed for reidentification**
The correct identification rates are rounded to the nearest whole number. The numbers at the end of the reidentification time plot represent the minimum amount of time sufficient for reidentification.

Discussion

This paper reviewed a vast literature base and summarised 72 studies. All but four of the included studies that reported CIR (n=57) had high CIR values (86–100%), suggesting that reidentification risks from wearable device data are higher than previously appreciated. Moreover, the minimum data duration for reidentification ranged from 1 to 300 s, suggesting that very small amounts of data can be sufficient to pose a privacy risk in seemingly anonymised biosensor data. All but four studies had fewer than 100 participants; thus, it remains to be seen whether these results would scale with larger populations. The few studies with larger participant pools (n=206–421; 4 studies) show results consistent with those with fewer participants (n=3–73; 68 studies), indicating that reidentification risks could remain a threat in larger group sizes. Further research is needed to determine to what extent large datasets pose similar risks for reidentification and what appropriate mitigation strategies are needed to protect privacy in large, public biosensor databases.

This systematic review highlights that, in many cases, reidentification requires very little data. For example, in a study with 46 participants,[26] 2 s of EEG recording could identify an individual with a CIR of 95%, and in another study with 51 participants[28] who were brushing their teeth while wearing an LG G watch (LG, Seoul, South Korea), 50 s of accelerometer and gyroscope data could identify an individual with a CIR of 96% (figure 5). This discovery is concerning since publicly available data is becoming increasingly abundant, especially given data-sharing advocacy and policy by influential bodies, such as the US Food and Drug Administration[36] and National Institutes of Health. We are also strong proponents of open science and open data to enable the use of FAIR[5] research principles and diverse representation. Thus, we find these results to be of concern and aim, with this systematic review, to bring the biomedical research community together to explore and discuss best practices to balance the potential risks and benefits of sharing versus not sharing data (figure 6). Consequently, the community must continue to re-evaluate data-sharing policies in the context of privacy and FAIR research principles as new studies become available on risks and benefits on both sides.

In general, our findings align with similar research on state-of-the-art non-wearable devices. For example, 12-lead ECG data[15] from two open access databases combined with other electronic health records data from 40 000 patients revealed CIR rates in similar ranges to those reported from studies we reviewed with wearable ECGs. The researchers looked at 37 heart conditions,

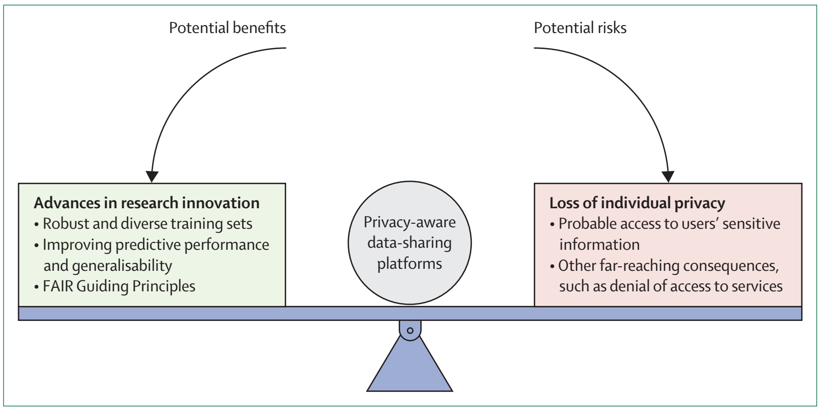

Potential benefits
Potential risks
Advances in research innovation
• Robust and diverse training sets
• Improving predictive performance and generalisability
• FAIR Guiding Principles
Privacy-aware data-sharing platforms
Loss of individual privacy
• Probable access to users' sensitive information
• Other far-reaching consequences, such as denial of access to services

Figure 6: **Benefits and risks of sharing data from wearable devices**
Potential benefits and potential risks of wearable device data sharing can tilt the benefit-risk balance either way. Privacy-aware data-sharing platforms can help to balance the benefits and risks. FAIR=Findable, Accessible, Interoperable, and Reusable.

including supraventricular tachycardia, ST depression, and pacing rhythm, and recorded an overall CIR of 94·56%. The CIR for individual conditions ranged from 90·32% to 98·55% in all but seven conditions. Patients with premature ventricular contractions had the lowest CIR of 78·54%.

In addition, 58% of the studies we analysed used head-worn and wrist-worn wearable devices (figure 4). This observation aligns with the global prediction for the wearable technology market[1] for 2026, which projects head-worn and wrist-worn wearable devices to have the most growth compared with wearable devices for other body locations.

Ultimately, it is necessary to possess identifiers to reidentify someone, so merely matching individuals in deidentified or anonymised datasets does not constitute true reidentification. Reidentification concerns have been historically dismissed because the probability that an attacker gains access to data containing identifiers has been believed to be low. However, an increasing number of companies are entering third-party data-sharing agreements,[37] some of which are ethically tenuous[37,38] (eg, driven by profits, personal benefit, or political gain over public good). The desire to know more about the patient or the customer and personalise goods and services by direct advertising is a likely culprit in reidentification attempts. For example, website scraping could reveal an individual's medical diagnoses and personality traits, which could be used to personalise advertising or reveal more information about the individuals to benefit the reidentifying entity (figure 1).

The findings here should not be used to justify blocking the sharing of biometric data from wearable devices. On the contrary, this systematic review exposes the need for more careful consideration of how data should be shared since the risk of not sharing data (eg, algorithmic bias[39,40] and failure to develop new algorithmic tools that could save lives) might be even greater than the risk of reidentification. Our findings suggest that privacy-preserving methods will be needed for open science to flourish. For example, there is an opportunity for regulatory bodies and funding agencies to expand support for privacy-conscious data-sharing platforms that mitigate reidentification risk. Such platforms could be, for instance, semi-public, research-focused, data-sharing platforms that only appropriately trained and approved researchers can access through two-way authentication schemes with organisational email addresses (eg, PhysioNet and AllOfUs). It should be noted, however, that systems like this could delay or even discourage some forms of citizen science. The community could also use new privacy-protecting methods, such as federated learning,[41] differential privacy,[42] and the use of synthetic data.[43]

On a different note, none of the studies we reviewed addressed the question of whether it is possible, in the absence of any identifying information about a group, to reidentify a person from that group with biosensor data alone. All included studies had a complete list of participants, which will not always be the case in many real-world scenarios. Therefore, there is a fundamental distinction between finding out which of the total study participants has the biometric signature of participant X versus obtaining X's name and telephone number without knowing who was in the study. In the case of genetic data, this is possible.[44] Could future investigators merge wearable-device public data with public genetic data to reidentify participants? Further study is needed to address this question.

Another limitation of this systematic review is that most studies had short session intervals or collected all data in one session. This limitation prevents drawing conclusions about template ageing (expected increases in error over time due to intraindividual changes—eg, changes in voice or face with age).[45,46] Because of template ageing, it might not be possible to identify individuals with data that is widely temporally spaced. Knowing maximum temporal intervals for any sensing modality with the ability to biometrically identify individuals could be an essential tool for policy makers. Once this is known, specific kinds of biometric data could be released to the public after scientifically determined temporal intervals. But with improving algorithms, these intervals might extend as well.

The included studies had substantial missing data (appendix p 1). For example, only 35% of studies mentioned anything about participants' health status; of these, only one participant was unhealthy, so the results from this systematic review might not be fully applicable to the broader population. However, if a disease is uncommon and easily identified with a biosensor, reidentifying an individual from the said sensor data would be straightforward. Future research should explore how health status affects biometric identification.

For more on **PhysioNet** see https://physionet.org/

For more on the **AllOfUs research project** see https://allofus.nih.gov/

We did not evaluate multimodal reidentification techniques in this systematic review; however, we anticipate multimodal reidentification to become more relevant in the near future.

In conclusion, a real risk of reidentification exists when wearable device sensor data is shared. Although this risk can be minimised, it cannot be fully mitigated. Our findings reveal that the basic practices of withholding identifiers from public repositories might not be sufficient to ensure privacy. More research is needed to guide the creation of policies and procedures that are sufficient to protect privacy, given the prevalence of wearable-device data collection and sharing. However, hope is not lost. The risk of not sharing data might be even greater than the risk of reidentification (eg, algorithmic bias[39,40] and failure to develop new algorithmic tools that could save lives), but new solutions are possible to reduce the risk of reidentification. For example, an emphasis on research directions for developing privacy-protecting methods (eg, federated learning,[41] differential privacy,[42] and the use of synthetic data[43]) could allow the biomedical research community to continue to reap the many benefits of data sharing while protecting the privacy of individuals.

Contributors

JD conceived the study. JD, DMG, LC, and YM designed the search strategy. LC retrieved all searches from the databases and exported them to Covidence. LC, YM, and DB participated in the title and abstract screening phase. LC, YM, MKW, and DB participated in the full-text review and data extraction phases. LC created all tables, graphs, and other visual representations, and YM and MKW participated in the quality assurance process for all tables, graphs, and visual representations. LC drafted the manuscript. All other authors read, edited, and approved the final manuscript.

Declaration of interests

JD is a scientific adviser with stock options at Veri; she received a grant from the Chan Zuckerberg Initiative, consulting fees from Gold Track, honoraria from the American College of Cardiology and Shionogi, and support for attending meetings (ICAMPAM 2022 and PMWC 2022). DMG is a scientific adviser for Magic Leap and Epilepsy AI; he has stock options with Magic Leap and has received gifts and services from Magic Leap. All other authors declare no competing interests.

Acknowledgments

The authors would like to express their gratitude to the engineering and computer science librarian at Duke University—Sarah Park. DMG is funded by NIH National Institute of Neurological Disorders and Stroke KL2TR002542. No funding was received for this study.

References

1 Markets and Markets. Wearable technology market. https://www.marketsandmarkets.com/Market-Reports/wearable-electronics-market-983.html?gclid=Cj0KCQjwgMqSBhDCARIsAIIVN1V0sqrk6SpYSga3rcDtWcwh8npZ08L0_s4X91gh7yPAa6QmsctB-lMaAlpqEALw_wcB (accessed April 10, 2022).

2 Cheung CC, Krahn AD, Andrade JG. The emerging role of wearable technologies in detection of arrhythmia. *Can J Cardiol* 2018; **34:** 1083–87.

3 Cheong SHR, Ng YJX, Lau Y, Lau ST. Wearable technology for early detection of COVID-19: a systematic scoping review. *Prev Med* 2022; **162:** 107170.

4 You L, Xu H, Zhang Q, et al. JDap: supporting in-memory data persistence in javascript using Intel's PMDK. *J Systems Archit* 2019; **101:** 101662.

5 Wilkinson MD, Dumontier M, Aalbersberg IJ, et al. The FAIR Guiding Principles for scientific data management and stewardship. *Sci Data* 2016; **3:** 160018.

6 Seh AH, Zarour M, Alenezi M, et al. Healthcare data breaches: insights and implications. *Healthcare* 2020; **8:** 133.

7 Greely HT. The uneasy ethical and legal underpinnings of large-scale genomic biobanks. *Annu Rev Genomics Hum Genet* 2007; **8:** 343–64.

8 Sweeney L. Weaving technology and policy together to maintain confidentiality. *J Law Med Ethics* 1997; **25:** 98–110.

9 Waldo A. A preliminary staff report on "protecting consumer privacy in an era of rapid change: a proposed framework for businesses and policymakers". https://www.ftc.gov/sites/default/files/documents/public_comments/preliminary-ftc-staff-report-protecting-consumer-privacy-era-rapid-change-proposed-framework/00300-57631.pdf (accessed July 27, 2022).

10 Richens JG, Lee CM, Johri S. Improving the accuracy of medical diagnosis with causal machine learning. *Nat Commun* 2020; **11:** 3923.

11 Shatte ABR, Hutchinson DM, Teague SJ. Machine learning in mental health: a scoping review of methods and applications. *Psychol Med* 2019; **49:** 1426–48.

12 Mehta Y, Majumder N, Gelbukh A, Cambria E. Recent trends in deep learning based personality detection. *Artif Intell Rev* 2020; **53:** 2313–39.

13 Bota PJ, Wang C, Fred ALN, Plácido Da Silva HA. Review, current challenges, and future possibilities on emotion recognition using machine learning and physiological signals. *IEEE Access* 2019; **7:** 140990–1020.

14 Henriksen-Bulmer J, Jeary S. Re-identification attacks—a systematic literature review. *Int J Inf Manage* 2016; **36** (6, part B)**:** 1184–92.

15 Ghazarian A, Zheng J, El-Askary H, Chu H, Fu G, Rakovski C. Increased risks of re-identification for patients posed by deep learning-based ECG identification algorithms. *Annu Int Conf IEEE Eng Med Biol Soc* 2021; **2021:** 1969–75.

16 Australian Bureau of Statistics. Understanding re-identification. 2021. https://www.abs.gov.au/about/data-services/data-confidentiality-guide/understanding-re-identification (accessed Nov 5, 2022).

17 Page MJ, McKenzie JE, Bossuyt PM, et al. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *Syst Rev* 2021; **10:** 89.

18 Maiorana E. A survey on biometric recognition using wearable devices. *Pattern Recognit Lett* 2022; **156:** 29–37.

19 Costache A, Badescu E, Popescu D, Ichim L. Identifying persons from iris image. 13th International Conference on Electronics, Computers and Artificial Intelligence (ECAI); July 1–3, 2021.

20 Qin Z, Huang G, Xiong H, Qin Z, Choo KKR. A fuzzy authentication system based on neural network learning and extreme value statistics. *IEEE Trans Fuzzy Syst* 2021; **29:** 549–59.

21 Brożek JL, Akl EA, Alonso-Coello P, et al. Grading quality of evidence and strength of recommendations in clinical practice guidelines. Part 1 of 3: an overview of the GRADE approach and grading quality of evidence about interventions. *Allergy* 2009; **64:** 669–77.

22 Guyatt GH, Oxman AD, Montori V, et al. GRADE guidelines: 5. Rating the quality of evidence—publication bias. *J Clin Epidemiol* 2011; **64:** 1277–82.

23 Kwon S, Kim H, Yeo WH. Recent advances in wearable sensors and portable electronics for sleep monitoring. *iScience* 2021; **24:** 102461.

24 Randazzo V, Cirrincione G, Pasero E. Shallow neural network for biometrics from the ECG-WATCH. In: Huang D-S, Bevilacqua V, Hussain A, eds. Intelligent computing theories and application. Berlin, Heidelberg: Springer-Verlag; 2020: 259–69.

25 Noh HW, Sim JY, Ahn CG, Ku Y. Electrical impedance of upper limb enables robust wearable identity recognition against variation in finger placement and environmental factors. *Biosensors* 2021; **11:** 398.

26 Zhang R, Yan B, Tong L, Shu J, Song X, Zeng Y. Identity authentication using portable electroencephalography signals in resting states. *IEEE Access* 2019; **7:** 160671–82.

27 Acar A, Aksu H, Uluagac AS, Akkaya K. A usable and robust continuous authentication framework using wearables. *IEEE Trans Mobile Comput* 2021; **20:** 2140–53.

28 Weiss GM, Yoneda K, Hayajneh T. Smartphone and smartwatch-based biometrics using activities of daily living. *IEEE Access* 2019; **7:** 133190–202.

29 Rahman KA, Alam N, Musarrat J, Madarapu A, Hossain MS. Smartwatch dynamics: a novel modality and solution to attacks on cyber-behavioral biometrics for continuous verification? 2020 International Symposium on Networks, Computers and Communications: Oct 20–22, 2020.

30 Sooriyaarachchi J, Seneviratne S, Thilakarathna K, Zomaya AY. MusicID: a brainwave-based user authentication system for internet of things. *arXiv* 2020; published online June 2. http://arxiv.org/abs/2006.01751 (preprint).

31 Ye C, Kumar BVKV, Coimbra MT. Human identification based on ECG signals from wearable health monitoring devices. 2011. https://doi.org/10.1145/2093698.2093723 (accessed May 19, 2022).

32 Pourbabaee B. Howe-Patterson M, Reiher E, Benard F. Deep convolutional neural network for ECG-based human identification. 2018. https://proceedings.cmbes.ca/index.php/proceedings/article/view/684 (accessed May 20, 2022).

33 Tao S, Zhang X, Cai H, Lv Z, Hu C, Xie H. Gait based biometric personal authentication by using MEMS inertial sensors. *J Ambient Intell Humaniz Comput* 2018; **9:** 1705–12.

34 Ferlini A, Ma D, Harle R, Mascolo C. EarGate: gait-based user identification with in-ear microphones. In: Proceedings of the 27th Annual International Conference on Mobile Computing and Networking [Internet]. New Orleans Louisiana: ACM; 2021 [cited 2022 May 15]. p. 337–49. Available from: https://dl.acm.org/doi/10.1145/3447993.3483240.

35 Sudhakar SRV, Kayastha N, Sha K, Act ID. An efficient framework for activity sensor based user identification. *Comput Secur* 2021; **108:** 102319.

36 Platt R, Brown JS, Robb M, et al. The FDA Sentinel Initiative—an evolving national resource. *N Engl J Med* 2018; **379:** 2091–93.

37 Fuller M. Big data and the Facebook scandal: issues and responses. *Theology* 2019; **122:** 14–21.

38 Schneble CO, Elger BS, Shaw D. The Cambridge Analytica affair and internet-mediated research. *EMBO Rep* 2018; **19:** e46579.

39 Starke G, De Clercq E, Elger BS. Towards a pragmatist dealing with algorithmic bias in medical machine learning. *Med Health Care Philos* 2021; **24:** 341–49.

40 Vayena E, Blasimme A, Cohen IG. Machine learning in medicine: addressing ethical challenges. *PLoS Med* 2018; **15:** e1002689.

41 Rieke N, Hancox J, Li W, et al. The future of digital health with federated learning. *NPJ Digit Med* 2020; **3:** 119.

42 Lv Z, Piccialli F. The security of medical data on internet based on differential privacy technology. *ACM Trans Internet Technol* 2021; **21:** 1–18.

43 Alzantot M, Chakraborty S, Srivastava M. SenseGen: a deep learning architecture for synthetic sensor data generation. 2017 IEEE International Conference on Pervasive Computing and Communications Workshops: March 13–17, 2017.

44 Gymrek M, McGuire AL, Golan D, Halperin E, Erlich Y. Identifying personal genomes by surname inference. *Science* 2013; **339:** 321–24.

45 Manjani I, Sumerkan H, Flynn PJ, Bowyer KW. Template aging in 3D and 2D face recognition. 2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems: Sept 6–9, 2016.

46 Matveev Y. The problem of voice template aging in speaker recognition systems. In: Železný M, Habernal I, Ronzhin A, eds. Speech and computer. Cham: Springer International Publishing, 2013: 345–53.