PERSPECTIVE
https://doi.org/10.1038/s41591-020-0994-1

nature medicine

Check for updates

# Regulatory, safety, and privacy concerns of home monitoring technologies during COVID-19

Sara Gerke[1]✉, Carmel Shachar[1], Peter R. Chai[2,3,4,5] and I. Glenn Cohen[6]

**There has been increasing interest in the use of home monitoring technologies during the COVID-19 pandemic to decrease interpersonal contacts and the resultant risks of exposure for people to the coronavirus SARS-CoV-2. This Perspective explores how the accelerated development of these technologies also raises major concerns pertaining to safety and privacy. We make recommendations for needed interventions to ensure safety and review best practices and US regulatory requirements for privacy and security. We discuss, among other topics, Emergency Use Authorizations for medical devices and privacy laws of the USA and Europe.**

Healthcare is increasingly shifting from the clinic to the home, where people are treated via telehealth services and are monitored for signs and symptoms with the help of smartwatches, apps, and other technologies that can be connected to a wireless network and/or can apply algorithms to the data obtained. For example, the elderly population — a vulnerable group — is growing in size[1], and with that growth, there is an increased need for the development of new digital health solutions so that people can live independent lives and be cared for at home for as long as possible.

The current COVID-19 pandemic has also accelerated the rate at which artificial intelligence and technologies are being integrated into healthcare in order to decrease exposure among healthcare and non-healthcare workers[2]. Social-distancing and quarantine measures have reduced the number of people with COVID-19 who need intensive in-hospital resources. Technology-assisted assessment of vital signs, such as pulse rate, body temperature, blood pressure, and respiration rate, can be used to assess home-isolated or quarantined people, provide basic care to others, and determine times at which home care may no longer be appropriate. It is hoped that mobile apps will aid in public-health measures such as contact tracing and enforced isolation of people who test positive for SARS-CoV-2.

The development of home monitoring technologies during this pandemic is being expedited to keep up with the demand. In particular, for better control of the spread of COVID-19, contact-tracing and warning apps have been implemented in several countries, such as Singapore, Austria, and Australia, and many more countries are developing such apps[3]. Apple and Google also launched their Exposure Notifications System, which enables local public-health authorities to identify, with the help of Bluetooth technology, potential exposures to COVID-19 and alert the exposed users to further instructions[4]. Contact-tracing apps rapidly notify users once they have had a close exposure to someone diagnosed with COVID-19 and prompts the users to self-quarantine or, in other cases, obtain testing for SARS-CoV-2[3]. While the term 'digital contact tracing' is often used in many instances, we think 'exposure notification' is the more accurate term. There is a strong incentive to use exposure-notification apps to alleviate some of the human labor that is needed for effective contract tracing.

We define a home monitoring technology as a product that is used for monitoring without (direct) supervision by a healthcare professional, such as in a patient's home, and that collects health-related data from a person. For example, an app that monitors the user's heart rate is considered a home monitoring technology. We understand 'home monitoring' to be an umbrella term for 'remote patient monitoring' and thus, for example, a device that remotely monitors a patient in a hospital without direct supervision by a healthcare professional meets our definition for this. In contrast, a telehealth visit is not considered a home monitoring technology, since there is a direct interaction between the patient and the healthcare professional. 'Health-related data' as we use the term can include health information, such as the user's heart rhythm, and/or non-health information that supports inferences about health, such as global-positioning-system data collected by exposure-notification apps[5]. The data collected by home monitoring technologies may be transmitted to healthcare professionals who then share relevant findings with their patients. However, it may also be the case that the home monitoring technologies' users and/or patients collect the data and may or may not decide to share such data with healthcare professionals or third parties.

Some home monitoring technologies are legally classified as medical devices, and others are not. To counter the COVID-19 pandemic, the US Food and Drug Administration (FDA) has begun using alternative pathways to permit medical devices to be brought to the market more quickly. However, the rapid development of new devices and other home monitoring products during this pandemic has brought additional risks. In this Perspective, we examine how to balance the need to make home monitoring technologies work in these times of emergency with two major concerns: safety and privacy. We also make recommendations on how to address these concerns.

## Safety concerns

**Classification of home monitoring technologies.** Some home monitoring technologies are classified as "medical devices" under

[1]The Petrie-Flom Center for Health Law Policy, Biotechnology, and Bioethics, Harvard Law School, Cambridge, MA, USA. [2]Department of Emergency Medicine, Brigham and Women's Hospital, Boston, MA, USA. [3]Department of Psychosocial Oncology and Palliative Care, Dana-Farber Cancer Institute, Boston, MA, USA. [4]Koch Institute for Integrative Cancer Research, Massachusetts Institute of Technology, Cambridge, MA, USA. [5]The Fenway Institute, Boston, MA, USA. [6]Harvard Law School, Cambridge, MA, USA. ✉e-mail: sgerke@law.harvard.edu

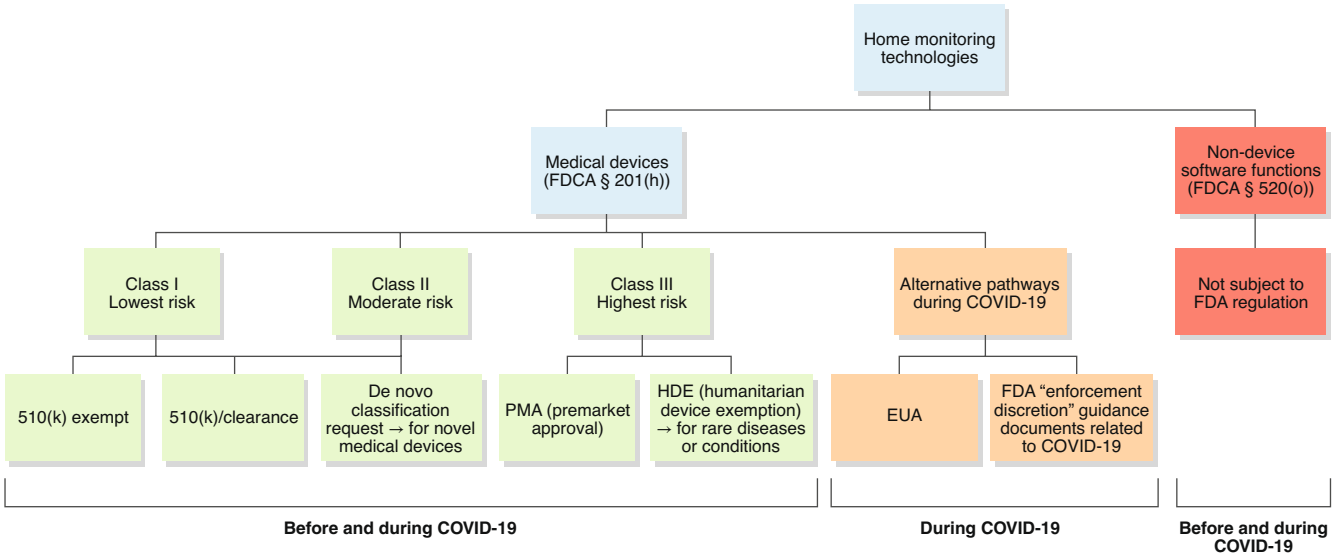


**Fig. 1 | Regulatory pathways of home monitoring technologies (before and) during the COVID-19 pandemic.** Blue shows that only some home monitoring technologies are legally classified as 'medical devices'. Green shows the various classes of medical devices (i.e., I, II, or III) based on their risk (from low to high); it also illustrates the usual premarket pathways for medical devices that were already available before the COVID-19 pandemic. Orange shows the two new regulatory pathways available for certain medical devices during the COVID-19 pandemic. Red shows that regardless of COVID-19, some home monitoring technologies are considered 'non-device software functions' and as such are not subject to FDA regulation.

Section (§) 201(h) of the US Federal Food, Drug, and Cosmetic Act (FDCA) since they are "intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease," do "not achieve its primary intended purposes through chemical action within or on the body of man" and are "not dependent upon being metabolized for the achievement of its primary intended purposes." Medical devices are classified into three classes (i.e., I, II, or III) on the basis of their risk (from low to high). The FDA usually reviews medical devices through different premarket pathways, depending on their risk classification (Fig. 1). Notably, software functions may also fulfill the device definition. The FDA refers to these as either 'Software in a Medical Device' or 'Software as a Medical Device'[6]. While the former is software that is an integral part of a hardware medical device, the latter is standalone software that as such is a medical device and is intended to be used for medical purposes[7,8]. For example, Apple launched an upgrade in 2018 to turn its watch into a personal electrocardiogram (ECG), which has enabled consumers to monitor their heart rhythm[9]. The FDA considered this app to be a moderate-risk device that requires special controls to provide reasonable assurance of its safety and effectiveness and thus classified this ' Software as a Medical Device' a class II device[10].

However, some home monitoring technologies are not considered medical devices and thus are not subject to FDA regulation. In particular, FDCA § 520(o), introduced by the 21st Century Cures Act, contains an exception from the device definition for certain software functions (Fig. 1). Examples would include an app that monitors users' food consumption to manage nutritional activity for weight management, or an app that exclusively monitors users' daily energy consumption and exercise activity to maintain and improve their good cardiovascular health[11].

The appropriate regulatory pathway is especially important during a pandemic, since there is pressure to speed up innovation but to not increase risk. The FDA has recently clarified that it does not consider most software systems and apps for public health surveillance to be medical devices[12]. In particular, the FDA noted that products that are intended to track contacts or locations associated with public health surveillance are usually not subject to FDA regulation since they generally do not fulfill the medical-device definition[12]. Consequently, the determination of whether the software function is considered a medical device is always made on a case-by-case basis.

**Emergency Use Authorizations for medical devices.** The US Secretary of Health and Human Services (HHS) determined on 4 February 2020 that there is a public-health emergency on the basis of the spread of SARS-CoV-2[13]. On the basis of this determination and to address the COVID-19 pandemic, the HHS secretary has issued three Emergency Use Authorization (EUA) Declarations related to medical devices. The first is for in vitro diagnostics for the diagnosis and/or detection of SARS-CoV-2[13], the second is for personal respiratory protective devices[14], and the most recent one broadly applies to medical devices, including alternative products that are used as medical devices, such as home monitoring devices[15].

So far, the FDA has already issued several EUAs for home monitoring devices ('EUA home monitoring devices') to address COVID-19[15,16] (Fig. 1 and Box 1). For example, an EUA was issued to G Medical Innovations for its VSMS patch intended to be used by healthcare professionals for remote patient monitoring of the QT interval of an ECG[17]. It is intended for use on patients over the age of 18 with COVID-19 who have been treated in hospitals with drugs that can cause life-threatening arrhythmias[17]. The patch, worn on the patient's upper left chest for up to 14 days, is linked to a smartphone, which then transmits the data to a call center, run by G Medical Innovations, for QT analysis. The clinical findings are compiled by a certified cardiographic technician and are subsequently sent to the doctor at the hospital[17]. It is also easily conceivable that similar devices could be deployed further. Indeed, in 2017, the VSMS patch received the CE mark — a precondition for bringing a device to market — in Europe for home use in patients[17].

It is likely that the FDA will issue more device-related EUAs in the coming weeks, including home monitoring technologies. However, authorization of home monitoring devices via the EUA pathway does give rise to potential risks. First, these are uncleared or unapproved medical devices or are cleared or approved devices for an uncleared or unapproved use. The FDA assesses these devices

**Box 1 | EUAs for medical devices under FDCA § 564**

The following are the major points that cover EUAs for medical devices during the COVID-19 pandemic and apply to home monitoring devices. Note that the scope and conditions of EUAs vary for each EUA, including labeling requirements, conditions related to advertising and promotion, etc. There may also be a possible waiver of certain FDA requirements, such as the requirements about current good manufacturing practice. An EUA is usually effective until it is revoked or the applicable HHS secretary's EUA Declaration is terminated.

Types of devices for which the FDA may issue EUAs:

- Uncleared or unapproved devices for commercial distribution
- Cleared or approved devices for an uncleared or unapproved use

Criteria for the issuance of EUAs in the context of the COVID-19 pandemic:

1. Serious or life-threatening disease or condition
   - SARS-CoV-2 can cause a serious or life-threatening disease or condition.
2. Evidence of effectiveness
   - "Based on the totality of scientific evidence", it is "reasonable to believe" that the device "may be effective" in treating, diagnosing, or preventing COVID-19.
3. Risk/benefit analysis
   - "Based on the totality of scientific evidence", it is "reasonable to believe" that the device's known and potential benefits outweigh its known and potential risks.
4. No alternatives
   - There is no available alternative to the device that is approved and adequate.
   - The criterion can be met if there is an approved alternative, but the supply of such an alternative is insufficient to fully cover the emergency needs[42].

on the basis of four criteria only (FDCA § 564(c)) (Box 1). In particular, one of the criteria is that there is a reasonable belief that the device may be effective in treating, diagnosing, or preventing COVID-19. Thus, the issuing of an EUA does not suggest that the product is safe or effective for monitoring[17]. Furthermore, another criterion for authorization is the performance of a risk/benefit analysis, and it is difficult to determine where to draw the cut-off for authorization on the basis of this type of analysis. Regulators should always make such decisions carefully and thoroughly, even in times of crisis. Second, when issuing an EUA, the FDA can waive certain requirements that usually help to reduce risks. For example, for the VSMS patch, the FDA waived the requirements for good manufacturing practice, which would be otherwise applicable[17]. However, such requirements have been developed to prevent harm to the end user and to minimize the risks involved in the manufacture of devices. It would thus be desirable that makers of EUA home monitoring devices build into their manufacturing process as many safeguards as possible to ensure that their products are safe as well as effective in fighting COVID-19.

There are also more-specific risks relating to EUAs for home monitoring devices. In particular, home monitoring technologies include a certain amount of false-positive and false-negative results, such as those caused by incorrect measurements or a failure to measure[18]. For example, a delay in treatment due to a failure of the device to detect a life-threatening cardiac arrhythmia may have disastrous consequences for a patient's health. This also raises questions of liability. When the particular circumstances and facts are taken into consideration, the Public Readiness and Emergency Preparedness (PREP) Act may provide liability immunity to a manufacturer of an EUA medical device[19,20]. But it is also crucial for manufacturers to understand that the FDA's nonbinding guidance documents for industry and FDA staff about enforcement discretion for certain medical devices related to COVID-19 (Box 2) do not bring such devices within the scope of the PREP Act[21] and thus do not provide immunity from liability.

Further risks of home monitoring technologies may include people's over-reliance on their output without seeking medical advice or the mishandling of such products by recipients — who have a greater range of mental and physical abilities and medical competency than clinicians do — in the absence of direct supervision by healthcare professionals[10,18]. In the case of Apple's ECG app, to mitigate the identified risks, the FDA explicitly required, among other things, rigorous clinical-performance and human-factors testing — a demonstration that the user can use the medical device correctly by only reading the labeling and can correctly interpret its output and comprehend when to seek medical help[10]. In contrast, the FDA has issued EUAs for home monitoring devices on the basis of, among other things, "reported clinical experience"[17,22,23]. We understand that new digital health solutions need to be deployed quickly to address the COVID-19 pandemic, in particular by reducing contacts between people. Nevertheless, to mitigate risks, companies should make sure, to the best of their ability, to test their products as rigorously as possible, such as by carrying out clinical- and non–clinical-performance testing and human-factors testing to demonstrate safe and effective product use by users in the USA[24]. This approach is also beneficial for companies in the long term, since an EUA is usually effective only until it is revoked or the applicable HHS secretary's EUA COVID-19 declaration is terminated (FDCA § 564(f)). Moreover, communication is key for avoiding over-reliance on EUA home monitoring devices, as well as their mishandling (Box 3).

**FDA-unregulated software functions.** Home monitoring technologies raise, in particular, safety issues, since some of them are not considered medical devices under FDCA § 201(h) and thus do not need to undergo any review by the FDA (Fig. 1). For example, if a COVID-19-exposure-notification app fails to notify a user of their potential exposure to COVID-19, this could result in the user's spreading the virus.

The risks noted above can be alleviated if device developers take an ethical approach. Ethics requires more than providing reasonable assurance that the product is safe and effective. In fact, technology companies should follow not only the principle of non-maleficence ('do no harm') but also principles of autonomy, beneficence, and justice[25]. Home health technologies need to be designed in a way that maximizes people's autonomy to the greatest extent possible while at the same time benefiting society and helping to tackle the current public-health emergency[26]. When developing these products, makers should, for example, ensure they mitigate biases and train their algorithms on unbiased data. They preferably should also work in interdisciplinary teams to reduce the risk of incorporating unconscious bias into the code. It is also essential that during the process of designing home monitoring technologies, technology companies adopt a system view rather than a product view[27]. A system view requires that companies, among other things, look at the context in which the home monitoring technology will be deployed (e.g., the home setting) and analyze the additional challenges that need to be overcome for successful implementation. For example, developers should consider the practical implementation aspects of home monitoring technologies, such as the need for users to have a wireless internet infrastructure. A system view also requires that

**Box 2 | Enforcement discretion by the FDA**

The FDA has issued several nonbinding guidance documents for industry and FDA staff about enforcement discretion for certain medical devices, including home monitoring technologies, related to COVID-19 in recent months[43] (Fig. 1). In particular, the FDA released an enforcement policy for non-invasive remote monitoring devices, including cardiac monitors, clinical electronic thermometers, electrocardiographs, oximeters, and breathing-frequency monitors[38]. The FDA clarified that for the duration of the public-health emergency, the legally marketed non-invasive remote monitoring devices listed in the new enforcement policy can be modified to a limited extent in their indications, functionality, claims, or software or hardware without the need to submit a 510(k) premarket notification, so long as they do not create an undue risk[38] (Fig. 1). For example, if the device has previously been marketed only for use in hospitals, it could now be modified for home use[38]. Other explicitly mentioned modifications in this policy include adding statements about patients with COVID-19 or changing the software or hardware of the device to improve remote monitoring capability[38].

The risks involved in the modifications will probably be generally lower than those of EUA home monitoring technologies, since these non-invasive remote monitoring devices have previously been legally marketed in the USA. Moreover, the FDA does intend to object to the limited modifications mentioned above if such modifications create an undue risk. An undue risk would, for example, involve a device that is intended to determine when a patient needs immediate clinical intervention[38].

Companies with legally marketed non-invasive remote monitoring devices that want to make limited modifications to their device to support patient monitoring during the COVID-19 pandemic should carefully read the FDA policy, with particular focus on whether their intended change creates an undue risk and the agency's labeling recommendations. In particular, if the device was initially marketed exclusively for use in clinical settings, companies should make sure to add user-friendly instructions for home use[38].

Another enforcement policy applies to uncleared clinical electronic thermometers (i.e., those that have not previously undergone FDA review), for which manufacturers would usually need to submit a 510(k) premarket notification[44]. Given the current public-health emergency, the FDA does not plan to object to the use and distribution of such uncleared devices, as long the performance and labeling elements laid down in the policy are met[44].

The diverse home monitoring devices covered by the various FDA enforcement discretion guidance documents have (slightly) different benefits and risks that the agency had to balance, taking into consideration the current threat posed by SARS-CoV-2. The FDA implemented these guidance documents without prior public participation, since the agency considered such participation "not feasible or appropriate"[43]. The reason may lie in the urgency of making more devices quickly available to mitigate contacts between healthcare professionals and patients. However, the public can still comment on such guidance documents[43].

**Box 3 | Best-practice recommendations for communication to recipients of EUA home monitoring devices**

Recipients should be given as much relevant information as possible, usually before they use the device[42]. The following is how we recommend that this be carried out, thereby taking into consideration the statutory requirements and the FDA's non-binding guidance on EUA of medical products[42].

All information should be typically provided in writing in the form of a fact sheet[42]. The fact sheet should be user-friendly, brief, and written in plain language[42]. The fact sheet should be preferably available in multiple languages to ensure that recipients who are not fluent in English are adequately informed.

The fact sheet should contain, in particular, the following information:

- The device's name[42]
- A description of the intended use of the device[42]
- An explanation of the disease (e.g., COVID-19)[42]
- A detailed explanation of what an EUA is, including its criteria for issuance and duration — in particular, it needs to be clearly communicated to the recipient that the device is authorized for emergency use only under an EUA by the FDA (FDCA § 564(e)) and that the device has not undergone the same type of FDA review as that for cleared or approved devices[18]; it should also be stated that the issuing of an EUA does not suggest that the device is safe or effective for monitoring
- Clear articulation to recipients of the significant potential and known benefits and risks of the device use, as well as the extent to which these benefits and risks are unknown (FDCA § 564(e)), especially the risks of false-positive and/or false-negative readings
- The recipient's general option to accept or refuse the device, as well as the consequences (if any) of such a refusal (FDCA, Section 564(e))
- Available alternatives to the device, including their benefits and risks (FDCA § 564(e))
- The duration of the monitoring
- An explanation of what type of data will be collected, who has access to such data, and with whom it will be shared and for what purposes
- A description of what privacy and security safeguards are in place to protect the recipient's privacy
- A description of the practical implementation aspects of the device (e.g., the need for a wireless internet infrastructure)
- A warning about over-reliance on the device's output, including an explanation of when to seek medical advice
- The 'dos and don'ts' of the use of the device to avoid its mishandling, including particular instructions for home use (if applicable)[42]
- Tips for further information (e.g., on EUAs, the product, COVID-19, etc.)

developers think about and address the interaction between the user and the product, the design interface, the accessibility of their products for all populations (so that they are immune to language barriers or to inaccessibility to those with disabilities), and issues of reimbursement and just allocation. For example, developers should consider the racial disparities that surround access to these technologies among vulnerable populations who may be most in need of these products. The FDA also developed non-binding guidance on "Design Considerations for Devices Intended for Home Use" that assists them in developing and designing home-use devices with appropriate standards of safety and effectiveness[28]. The European Commission's High-Level Expert Group on Artificial Intelligence also has Ethics Guidelines for Trustworthy Artificial Intelligence[29].

More work still needs to be done for better understanding and articulation of how to achieve the goal of designing 'trustworthy'

digital health solutions such as home monitoring technologies. It will be vital to develop ethical guidelines tailored explicitly to home monitoring technologies by involving all stakeholders in the field — in particular, the users of such products. Health psychology may also serve as a useful tool for guiding the design of home monitoring technologies[26]. During this pandemic, speeding up of the development of home monitoring products has been indispensable, but developers should not forget to continue to practice 'ethics by design' without making too many trade-offs[30], to continuously monitor these products[31] and adjust them where necessary, to learn from mistakes, and to improve and develop a 'gold standard' after the pandemic. Technology companies should also be aware that tort claims by users that home monitoring products that are not classified as medical devices are defective will probably be governed under product liability law and that there is no immunity under the PREP Act.

**Fraudulent home monitoring products.** Unfortunately, some companies' goal is to make a profit during this public-health emergency with indifference to patient and/or user welfare. The FDA has already warned consumers against fake medical products that claim to treat, prevent, or cure COVID-19, such as unauthorized vaccines or home test kits[32]. The US Federal Trade Commission is also warning consumers to avoid coronavirus scams, including ignoring online offers for home test kits and vaccinations[33].

It is essential that consumers be adequately protected from fraudulent home monitoring products. State attorneys general should monitor this area closely and bring consumer-protection-act claims when appropriate. Clinicians can also help to educate patients and warn them about particular fraudulent products in the field.

## Privacy concerns

Home monitoring technologies raise privacy concerns, since they collect people's health-related data that are sensitive and need to be adequately protected. Proper privacy protection is important for respect for a person's autonomy and also for building and promoting trust. If people do not have trust in technology companies as builders of home monitoring technologies, they will refuse to use them. This could be fatal because, for example, exposure-notification apps can be effective only if enough people voluntarily use them. Thus, manufacturers of home monitoring technologies not only should comply with the applicable privacy and security laws but also should be keen on implementing the best fundamental ethical practices for privacy in the development process of their products, to facilitate trust.

**Privacy laws in the USA and Europe.** The personal data of European users of home monitoring technology is probably already protected by European Union (EU) General Data Protection Regulation (GDPR) 2016/679 and by the EU member states' laws that implemented the ePrivacy Directive (2002/58/EC), in most cases. For example, the GDPR prohibits the processing of special categories of personal data, such as data concerning health and genetic data (Article 9(1)). However, this regulation also contains a few exceptions to this general ban (Article 9(2)), including one for public-interest reasons in the area of public health that may serve as a legal ground for the processing of such sensitive data in the context of pandemics such as COVID-19 (Article 9(2)(i))[34]. The ePrivacy Directive that has been transposed into the national law of the EU member states also provides safeguards for electronic communication data, such as location data from mobile phones[34].

The EU GDPR that became applicable on 25 May 2018 is a much newer data-protection scheme than the key federal health data privacy law in the USA, the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The GDPR includes several principles and rights of people whose personal data are processed, such as the principle of lawfulness, fairness, and transparency (Article 5(1)(a)) or the right to be forgotten (Article 17). The GDPR has also inspired some US states to introduce similar privacy law bills, most prominently the California Consumer Privacy Act (CCPA) of 2018 that became effective on 1 January 2020. Further, the GDPR has a broad territorial scope and may apply under certain circumstances even to companies not established in the EU, such as in cases in which they process the personal data of subjects who are in the EU and the processing activities are related to the targeted "monitoring of their behaviour as far as their behaviour takes place within the Union" (Articles 3(2)(b) and 4(1))[35]. US developers should thus consider designing their home monitoring technologies to comply with GDPR requirements.

In April 2020, the European Commission announced an EU toolbox for the use of contact-tracing and warning apps, developed by the EU member states with the support of the commission[36]. This toolbox aims to provide the EU member states with practical guidance in the implementation of such apps, including key requirements for them[36]. In particular, the contact-tracing and warning apps "should be fully compliant with the EU data protection and privacy rules," "should be installed voluntarily," "should aim to exploit the latest privacy-enhancing technological solutions," such as (preferably) the use of Bluetooth proximity technology rather than location data, and "should be based on anonymised data"[36]. While this toolbox is specific to contact tracing in the EU, the requirements can and should be used by US developers and should be extended to all home monitoring technologies. Public-health authorities should also make sure to include the most vulnerable groups to benefit from new home monitoring technologies.

By contrast, in the USA, existing privacy regulations address the questions raised by home monitoring technologies only somewhat. The HIPAA Privacy Rule governs, in general, the use and disclosures of protected health information — which is, in general, "individually identifiable health information" (Code of Federal Regulations (CFR): 45 CFR § 160.103). From the outset, however, HIPAA applies to such health information only if it is generated by "covered entities," such as most healthcare providers, or their "business associates." Thus, most technology companies fall outside of HIPAA's purview[5], and the information their home monitoring products (such as apps) gather may be unprotected. This blind spot would allow these companies to freely share the data they collect on people. Some uses may be bona fide and largely beneficent, such as providing data to contact-tracing programs to better manage a crisis, but other uses may be more objectionable, such as commercializing the data gathered from patients. Sometimes state law addresses this gap. The CCPA provides Californians with some privacy protections, such as requiring particular companies to delete a consumer's personal information when requested (California Civil Code § 1798.105). However, many other states still need to catch up, and US users of home monitoring technology should be warned that their privacy may not be protected. In general, the USA would benefit from a federal law that provides protection similar to that provided by the EU GDPR to ensure that people in in all states of the USA have proper privacy protection.

Individually identifiable home-monitoring health information entered into an electronic health record (EHR) becomes HIPAA-protected health information. HIPAA contains certain exceptions for covered entities to use or disclose protected health information, such as for public-health activities (45 CFR § 164.512(b)) and health-oversight activities (45 CFR § 165.512(d)). For example, this would cover a physician's electronically transmitting a cluster of high temperature readings to the local public-health authorities for the purpose of controlling or preventing COVID-19, or their sending data in the EHR from home monitoring products to states' contact-tracing programs. Furthermore, the Office for Civil Rights at HHS announced in April 2020 that it will also not

impose possible penalties for violations of certain HIPAA rules against business associates or covered entities in cases in which business associates use or disclose protected health information for public-health activities (consistent with 45 CFR § 164.512(b)) or health-oversight activities (consistent with 45 CFR § 165.512(d)) during this pandemic[37]. Business associates are usually allowed to use or disclose protected health information for such purposes only if this is explicitly permitted in their business associate agreement (BAA) with the covered entity[37]. However, the Office for Civil Rights will exercise its enforcement discretion only where the business associates act in good faith and notify the covered entity within 10 calendar days after the disclosure or use occurs[37].

The HIPAA Security Rule contains security standards for protecting electronic protected health information. The healthcare sector has heightened vulnerability to cyber attacks, and these incidents can lead to suboptimal care or harm to people. In cases of limited modifications to the software or hardware of certain non-invasive remote monitoring devices, the FDA also recommended in its enforcement policy that manufacturers implement suitable cybersecurity controls to maintain device safety and functionality as well as to ensure device cybersecurity[38]. Cybersecurity vetting can take months, especially for newer products, which could prevent the rapid deployment of these technologies when they are most needed. The use of Bluetooth technology for exposure notification, for example, is far less invasive than the collection of WiFi or global-positioning-system location data, but Bluetooth is also known to be vulnerable to cyber attacks[39,40].

**Best fundamental ethical practices for privacy.** Home monitoring technologies represent a new and potentially problematic incursion into the privacy of people. Because of the heightened privacy expectations, especially in the users' home, it is important that technology companies, healthcare provider**s**, and public-health officials operate with the highest ethical standards, in particular when the existing privacy regulations do not apply. This includes the utilization of anonymized data whenever possible (and otherwise preferably with people's consent) and having safeguards in place for re-identification risk[41]. In general, people should be given the choice to use home monitoring technologies and should be expressly asked to 'opt in'. They should also be able to 'opt out' and to stop sharing their home monitoring data at any time. Further, all people in the USA should have a 'right to be forgotten' similar to the one in the EU GDPR, whereby people can usually request the erasure of their personal data (Article 17), and the CCPA (California Civil Code § 1798.105(a)). To avoid undermining data analysis efforts and to keep governance of these technologies similar to the CCPA, the right to be forgotten should be limited to personal information and should not be extended to de-identified or aggregate consumer information (California Civil Code § 1798.140(o)).

The use of home-monitoring data beyond direct patient treatment or user application, especially connected to COVID-19 surveillance efforts, should be transparent. This will allow people the opportunity to decide if they find this use permissible or if they want to avoid the application of these technologies. For example, an app that exclusively monitors users' daily energy consumption and exercise activity to maintain and improve their good cardiovascular health[11] during the COVID-19 pandemic should, among other things, transparently inform users whether and for what purposes their data will be shared with third parties. The commercial use of data from home monitoring products should also be banned, unless the use is stated very clearly up front and people can still use the product even if they refuse to consent to the commercial use of their data. In general, as long as there is no new federal law in the USA that protects all health-related data, individually identifiable data generated by home monitoring products should either be stored in the patients' medical records or be covered by BAAs — where the data will receive HIPAA's protections — or should be stored in the users' device or smartphone rather than on remote servers. This data architecture will limit invasion of privacy by preventing easy access to the data.

There is also more work to be done when it comes to the equitable application of home monitoring technologies. Monitoring requires access to technologies such as a smartphone or other devices, and this fact raises ethical questions about whether current health disparities will be further increased rather than being mitigated. To its credit, the European Commission, for example, has recognized this issue in the context of digital contact tracing (or, as we call it, 'exposure notification') and has explained that "manual tracing will continue to cover citizens who could be more vulnerable to infection but are less likely to have a smartphone, such as elderly or disabled persons"[36]. However, home monitoring products may be the most useful for these vulnerable people. Efforts should be made by public-health authorities to include the most vulnerable groups to benefit from new home monitoring technologies.

**Best US regulatory practices for privacy and security.** In the current public health emergency, US healthcare providers and technology companies should make sure — to the best of their ability — to comply with HIPAA and protect people's privacy. As a best practice, developers should try to incorporate HIPAA's requirements, such as encryption, into their home monitoring even when HIPAA does not directly apply to their products. Entities governed by HIPAA, such as hospitals, seeking to collaborate with non–HIPAA-covered technology companies typically enter into BAAs. BAAs usually contain proper safeguards on the disclosure and use of HIPAA-protected health information. The negotiation and finalizing the setting-up of BAAs, however, can be time-consuming — valuable time that the parties probably do not have during this public-health emergency. Thus, to promote the execution of BAAs during the COVID-19 pandemic and for the sake of people's privacy, HHS should consider creating a temporary BAA for stakeholders looking to implement home monitoring technologies for combating COVID-19 to be used during this pandemic. Unique terms for the COVID-19 BAA could include minimum privacy standards, additional time to report to covered entities or to respond to people' requests for access, and expanded ability to disclose information for public-health purposes.

Likewise, HHS should create a rapid process for cybersecurity vetting of new home health technologies used to combat COVID-19. To balance security concerns with the need to act swiftly, HHS should establish guidance on the basic minimum cybersecurity standards needed during the COVID-19 pandemic. This best-practice guidance should both facilitate the rapid implementation of new products and articulate, among other things, the preferred technology to use (e.g., Bluetooth proximity technology), security measures to mitigate cyber-attacks, and a protocol for a fast response to any vulnerabilities uncovered, including recalling products when necessary.

## Conclusions

Home monitoring technologies have considerable potential to decrease personal contacts between people and thus exposure to COVID-19. However, the rapid development of new products also poses challenges ranging from safety and liability to privacy. The motto 'ethics by design, even in a pandemic' should guide makers in the development of home monitoring products to combat this public-health emergency.

Received: 16 April 2020; Accepted: 24 June 2020;
Published online: 7 August 2020

## References


1. Centers for Medicare & Medicaid Services. CMS Fast Facts. https://www.cms.gov/Research-Statistics-Data-and-Systems/ Statistics-Trends-and-Reports/CMS-Fast-Facts/index (2020).
2. Wittbold, K.A. et al. How hospitals are using AI to battle Covid-19. *Harvard Business Review* https://hbr.org/2020/04/how-hospitals-are-using-ai-to-battle-covid-19 (2020).
3. Cohen, I.G., Gostin, L.O. & Weitzner, D.J. Digital smartphone tracking for COVID-19: public health and civil liberties in tension. *J. Am. Med. Assoc.* **323**, 2371–2372 (2020).
4. Google. Exposure notifications: using technology to help public health authorities fight COVID-19. https://www.google.com/covid19/exposurenotifications/ (2020).
5. Price, W. N. II & Cohen, I. G. Privacy in the age of medical big data. *Nat. Med.* **25**, 37–43 (2019).
6. FDA. Policy for device software functions and mobile medical applications. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/policy-device-software-functions-and-mobile-medical-applications (2019).
7. FDA. Software as a Medical Device (SaMD). https://www.fda.gov/medical-devices/digital-health/software-medical-device-samd (2018).
8. IMDRF. Software as a Medical Device (SaMD): key definitions. http://www.imdrf.org/docs/imdrf/final/technical/ imdrf-tech-131209-samd-key-definitions-140901.pdf (2013).
9. Apple. ECG app and irregular heart rhythm notification available today on Apple Watch. https://www.apple.com/newsroom/2018/12/ecg-app-and-irregular-heart-rhythm-notification-available-today-on-apple-watch (2018).
10. FDA. Letter to Apple Inc. https://www.accessdata.fda.gov/cdrh_docs/pdf18/DEN180044.pdf (2018).
11. FDA. Changes to existing medical software policies resulting from section 3060 of the 21st Century Cures Act. https://www.fda.gov/media/109622/download (2019).
12. FDA. Digital health policies and public health solutions for COVID-19. https://www.fda.gov/medical-devices/digital-health/digital-health-policies-and-public-health-solutions-covid-19 (2020).
13. Federal Register. HHS Determination of public health emergency 85 FR 7316. https://www.federalregister.gov/documents/2020/02/07/2020-02496/determination- of-public-health-emergency (2020).
14. Federal Register. HHS Emergency Use Declaration 85 FR 13907. https://www.federalregister.gov/documents/2020/03/10/2020-04823/emergency-use-declaration (2020).
15. Federal Register. HHS Emergency Use Authorization Declaration 85 FR 17335. https://www.federalregister.gov/documents/2020/03/27/2020-06541/emergency-use-authorization-declaration (2020).
16. FDA. Remote or wearable patient monitoring devices EUAs. https://www.fda.gov/medical-devices/coronavirus-disease-2019-covid-19-emergency-use-authorizations-medical-devices/remote-or-wearable-patient-monitoring-devices-euas?utm_campaign=2020-06- 18%20New%20EUA%20COVID-19%20page&utm_ medium=email&utm_source=Eloqua (2020).
17. FDA. Letter to G Medical Innovations Ltd. https://www.fda.gov/media/138105/download (2020).
18. FDA. Fact sheet for healthcare providers: G Medical VSMS ECG patch. https://www.fda.gov/media/138104/download (2020).
19. Federal Register. HHS Declaration under the Public Readiness and Emergency Preparedness Act for medical countermeasures against COVID-19 85 FR 15198. https://www.federalregister.gov/documents/2020/03/17/20-20-05484/declaration-under-the- public-readiness-and-emergency-preparedness-act-for-medical-countermeasures (2020).
20. HHS. Advisory opinion on the Public Readiness and Emergency Preparedness Act and the March 10, 2020 Declaration under the Act April 17, 2020, as modified on May 19, 2020. https://www.hhs.gov/sites/default/files/prep-act-advisory-opinion-hhs-ogc.pdf (2020).
21. Spivack, P.S. & Lyons, E.M. Liability immunity under the PREP Act for COVID-19 countermeasures: what manufacturers need to know. https://www.hoganlovells.com/~/media/hogan-lovells/pdf/2020-pdfs/2020_03_23_liability_immunity_under_the_prep_act-for _covid_19_countermeasures.pdf (2020).
22. FDA. Letter to Elite BioMedical Consultant, Inc. https://www.fda.gov/media/137693/download (2020).
23. FDA. Letter to VitalConnect, Inc. https://www.fda.gov/media/137397/download (2020).
24. FDA. Applying human factors and usability engineering to medical devices. https://www.fda.gov/media/80481/download (2016).
25. Beauchamp, T.L. & Childress, J.F. *Principles of Biomedical Ethics* (New York: Oxford University Press, 2012).
26. Calvo, R. A., Deterding, S. & Ryan, R. M. Health surveillance during covid-19 pandemic. *Br. Med. J.* **369**, m1373 (2020).
27. Gerke, S., Babic, B., Evgeniou, T. & Cohen, I. G. The need for a system view to regulate artificial intelligence/machine learning-based software as medical device. *NPJ Digit. Med.* **3**, 53 (2020).
28. FDA. Design considerations for devices intended for home use. Guidance for industry and Food and Drug Administration Staff. https://www.fda.gov/media/84830/download (2014).
29. European Commission's High-Level Expert Group on Artificial Intelligence. Ethics guidelines for trustworthy AI. https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai (2020).
30. Gerke, S., Minssen, T., Yu, H. & Cohen, I. G. Ethical and legal issues of ingestible electronic sensors. *Nat. Electron.* **2**, 329–334 (2019).
31. Babic, B., Gerke, S., Evgeniou, T. & Cohen, I. G. Algorithms on regulatory lockdown in medicine. *Science* **366**, 1202–1204 (2019).
32. FDA. Beware of fraudulent coronavirus tests, vaccines and treatments. https://www.fda.gov/consumers/consumer-updates/beware-fraudulent-coronavirus-tests-vaccines-and-treatments?utm_campaign=CU%20Roundup%20040320&utm_medium=email&utm_source=Eloqua (2020).
33. Federal Trade Commission. Consumer information. Coronavirus. https://www.consumer.ftc.gov/features/coronavirus-scams-what-ftc-doing (2020).
34. European Data Protection Board. Statement by the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak. https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_en (2020).
35. European Data Protection Board. Guidelines 3/2018 on the territorial scope of the GDPR (Article 3). Version 2.0. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en.pdf (2019).
36. European Commission. Coronavirus: An EU approach for efficient contact tracing apps to support gradual lifting of confinement measures. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_670 (2020).
37. Federal Register. HHS enforcement discretion under HIPAA to allow uses and disclosures of protected health information by business associates for public health and health oversight activities in response to COVID-19 85 FR 19392. https://www.federalregister.gov/documents/2020/04/07/2020-07268/enforcement-discretion-under-hipaa -to-allow-uses-and-disclosures-of-protected-health-information-by (2020).
38. FDA. Enforcement policy for non-invasive remote monitoring devices used to support patient monitoring during the coronavirus disease-2019 (COVID-19) public health emergency. Guidance for industry and Food and Drug Administration Staff. https://www.fda.gov/media/136290/download (2020).
39. Privacy International. Bluetooth tracking and COVID-19: A tech primer. https://privacyinternational.org/explainer/3536/bluetooth-tracking-and-covid-19-tech-primer (2020).
40. Becker, J. K., Li, D. & Starobinski, D. Tracking anonymized Bluetooth devices. *Proc. Priv. Enhancing Technol.* **3**, 50–65 (2019).
41. Gerke, S., Yeung, S. & Cohen, I. G. Ethical and legal aspects of ambient intelligence in hospitals. *J. Am. Med. Assoc.* **323**, 601–602 (2020).
42. FDA. Emergency use authorization of medical products and related authorities. Guidance for industry and other stakeholders. https://www.fda.gov/media/97321/download (2017).
43. FDA. Coronavirus (COVID-19) and Medical Devices. https://www.fda.gov/medical-devices/emergency-situations-medical- devices/coronavirus-covid-19-and-medical-devices (2020).
44. FDA. Enforcement policy for clinical electronic thermometers during the coronavirus disease 2019 (COVID-19) public health emergency. https://www.fda.gov/media/136698/download (2020).


## Acknowledgements

S.G., C.S., and I.G.C. were supported by a grant from the Collaborative Research Program for Biomedical Innovation Law, a scientifically independent collaborative research program supported by a grant NNF17SA0027784 from Novo Nordisk Foundation. P.R.C. is supported by grant NIH K23DA044874, NIH R44DA051106, and investigator initiative research from e-ink corporation and the Hans and Mavis Lopater Psychosocial Foundation.

## Competing interests

I.G.C. served as a bioethics consultant for Otsuka on their Abilify MyCite product and is a member of the Illumina Ethics Advisory Board.

## Additional information

**Correspondence** should be addressed to S.G.