OPEN ACCESS

ORIGINAL RESEARCH

# Protecting patient privacy in digital health technology: the Dutch m-Health infrastructure of Hartwacht as a learning case

Eric Wierda ,[1,2] Sebastiaan Blok,[3] G Aernout Somsen,[3] Enno T van der Velde,[4] Igor I Tulevski,[3] Borut Stavrov,[3] Maud C C de Wildt,[3] Bert J H van den Born,[5] Laura Breukel,[6] Bas A J M de Mol,[7] M Corrette Ploem,[8] Michiel M Winter[1]

For numbered affiliations see end of article.

**Correspondence to**
Dr Eric Wierda, Department of Cardiology, Dijklander Hospital, Maelsonstraat 3, 1624 NP, Hoorn, The Netherlands; e.wierda@amsterdamumc.nl

EW and SB are joint first authors.
MCP and MMW are joint last authors.

Received 2 October 2019
Revised 7 April 2020
Accepted 2 June 2020
Published Online First 2 July 2020



**To cite:** Wierda E, Blok S, Somsen GA, *et al*. *BMJ Innov* 2020;**6**:170–176.

## ABSTRACT

Innovative ways of healthcare delivery like m-Health, the practice of medicine by mobile devices and wearable devices are the promising new technique that may lead to improvement in quality of care at lower costs. While fully acknowledging the importance of m-Health development, there are challenges on privacy legislation. We address the legal framework, especially the General Data Protection Regulation, applied to m-Health and its implications for m-Health developments in Europe. We discuss how these rules are applied using a representative example of an m-Health programme with remote monitoring in the Netherlands. We consider informing patients about the data processing and obtaining their explicit consent as main responsibilities of healthcare providers introducing m-Health in their practice.

## INTRODUCTION

Healthcare systems worldwide are facing new challenges, such as an ageing population, inadequate delivery of medical resources and increasing budgetary pressure.[1] Innovative ways of healthcare delivery, such as mobile health (m-Health), are rapidly gaining ground in the pursuit to face these challenges. m-Health is a subtheme of e-Health (the use of Information Communciation Technology (ICT) in health)[2 3] and is defined as the practice of medicine by mobile devices (ie, mobile phones and tablets) and wearable devices (ie, smart watches, mobile single lead ECGs).[4 5] Monitoring patients outside a hospital with m-Health is likely to increase patient's health status at decreased expenditure.[6] Although m-Health is promising, it poses important challenges on privacy, data protection and data security.[7]

In 2016, the parliament of the European Union (EU) adopted the General Data Protection Regulation (GDPR), which came into force in May 2018.[8 9] Already in 2012, the European Commission of the EU proposed a comprehensive reform of the earlier EU's privacy directive (Directive 95/46/EC, dating back to 1995). In light of the rapid digitalisation, a strong and more coherent data protection framework was considered necessary to protect individuals with regard to the processing and free movement of their personal data. Since m-Health depends heavily on the collection, storage, transfer and interpretation of patients' personal (health) data, each m-Health infrastructure, set up within the EU's territorial scope (Article 3 GDPR), should be in accordance with the GDPR's provisions.[5] The scope of the Regulation includes all data processing carried out by a medical centre or company based in the EU. Ensuring GDPR compliance is important to safeguard legitimate data processing, and to keep the confidence of patients who entrust their data and privacy to their doctors. Institutions that use personal data and fail to comply can face penalties that can be up to 4% of previous year's turnover.[10]

In a responsible m-Health infrastructure, all data processing should meet

the requirements of the GDPR. To facilitate further m-Health development in the EU, we provide a comprehensible step-by-step roadmap on how to set up a GDPR-proof m-Health infrastructure. As an example, we provide our own m-Health infrastructure that was recently introduced in the Netherlands (HartWacht). We examine the challenges we encountered with regard to HartWacht and the GDPR. Finally, we discuss possible pitfalls healthcare providers should be aware of when introducing a GDPR-compliant m-Health infrastructure.

## HARTWACHT: A DUTCH EXAMPLE OF AN M-HEALTH INFRASTRUCTURE

In 2016, Hartwacht—a system to monitor patients with widespread heart diseases—was introduced in the Netherlands. It enables patients to perform health measurements at home. The programme is set up for three patient groups: patients with cardiac arrhythmias, patients with hypertension and patients with congestive heart failure. Cardiology Centres of the Netherlands (CCN) serves as healthcare provider (HCP). Devices (hardware) and applications (software) are provided by several partners. The devices are connected to the applications for smartphone, tablet or personal computer. Collected health data are transferred to CCN, through partner servers and integrated in the electronic patient files. Incoming health data are interpreted by dedicated nurses under the supervision of a cardiologist. If necessary, this team contacts the patient or the treating physician (see figure 1).

### Data processing within HartWacht

For proper functioning of the Dutch heart disease surveillance system, large amounts of personal health data need to be collected, stored, transferred, shared and interpreted. Figure 2 shows an overview of data processing within Hartwacht. For each of these phases different articles from the GDPR are applicable. We will describe every phase with its corresponding relevant GDPR articles and show the experience of HartWacht in complying with GDPR. An overview is presented in table 1.

## IMPLICATIONS OF GDPR FOR M-HEALTH INFRASTRUCTURES

### Compliance with GDPR

In May 2018, the GDPR came into force with as its main goal to offer protecting to all EU-citizens with respect to the processing of their personal data.[8] The GDPR has consequences for the emerging field of m-Health, which is almost completely dependent on the processing of health data. It is the responsibility of each HCP initiating an m-Health programme '(…) to ensure and to be able to demonstrate that processing is performed in accordance with (…) (the GDPR)', this by implementing appropriate technical and organisational measures to secure the data processing (Article 24 paragraph 1 GDPR).

Health data are identified in the GDPR as a 'special category'. This means they are protected by a stricter privacy regime than other, 'regular', data.[11 12] Health data are broadly defined as 'data related to the physical or mental health of a natural person' (Article 4 GDPR), and this clearly includes data on someone's physical condition collected with mobile and/or wearable devices.[8] As misuse of health data can have severe and extensive consequences for individuals, the processing of such data is prohibited, with only few exceptions (Article 9 GDPR).

In light of the GDPR, three 'stakeholders' are relevant in an m-Health home monitoring infrastructure.

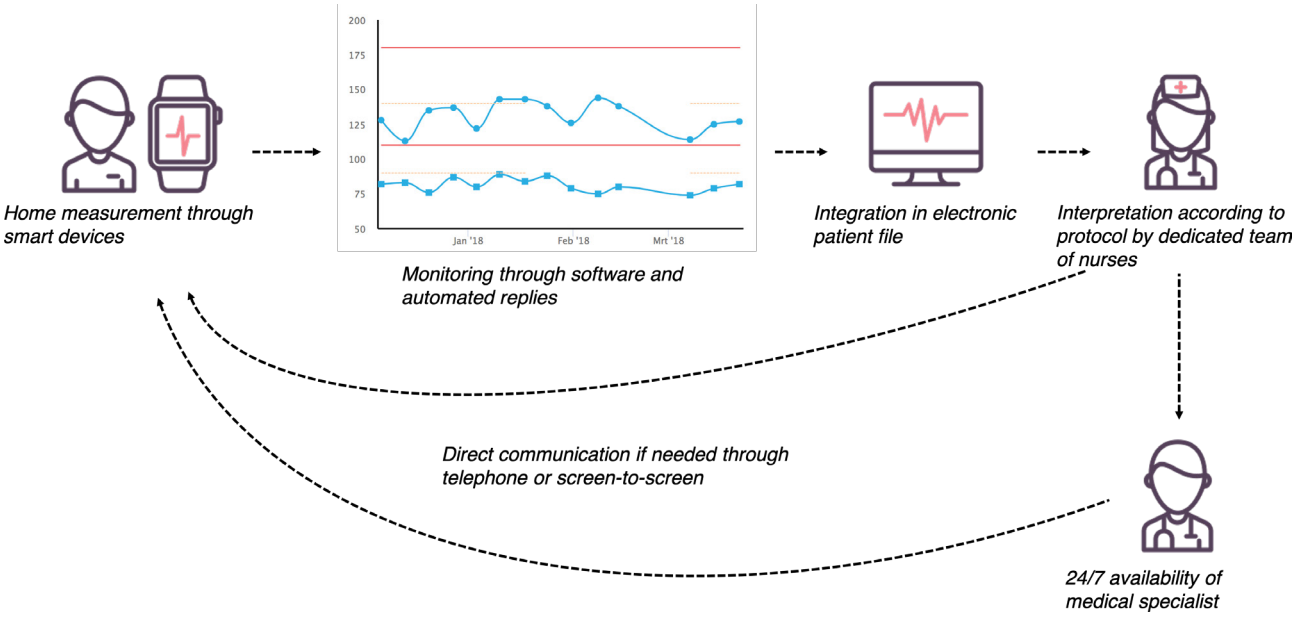


**Figure 1** The mHealth infrastructure of HartWacht.

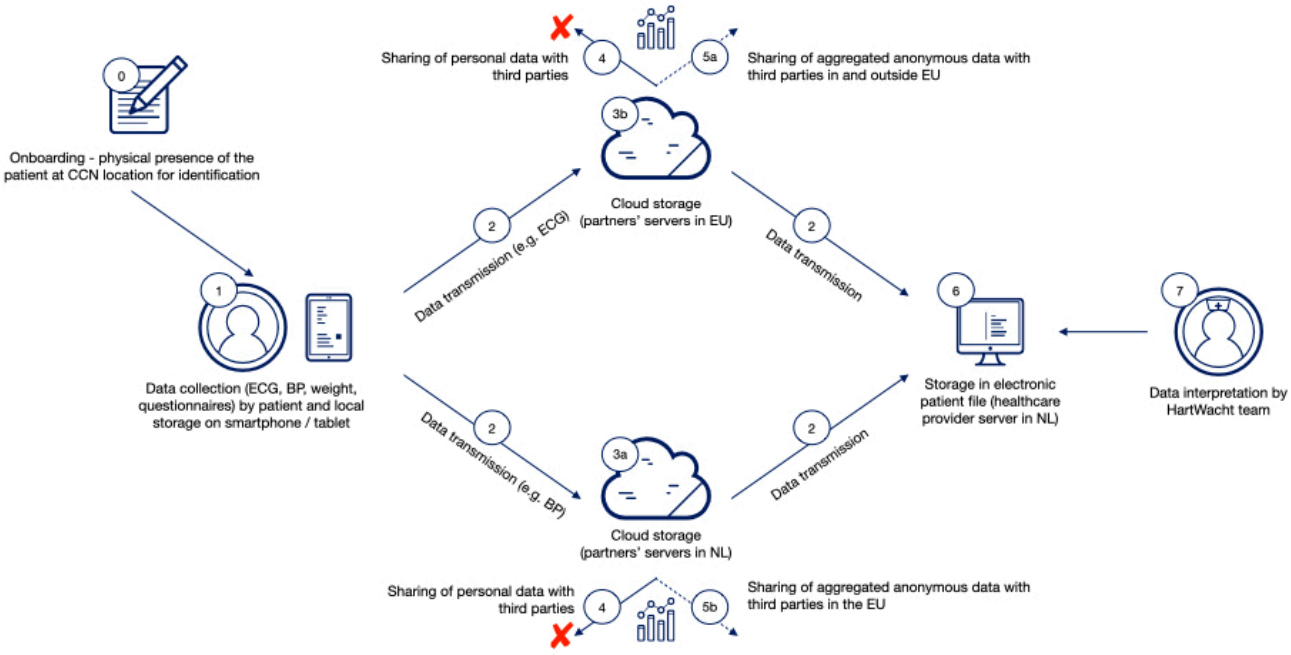


**Figure 2** Data processing in mHealth home monitoring infrastructure (HartWacht).

First, the data subject (hereafter 'the patient'): a person that can be identified through the data that are used in m-Health and whose rights are protected in the regulation (Article 4 paragraph 1 GDPR). Second, the data controller (hereafter 'the healthcare provider' or HCP): the institution, and on its behalf, the responsible healthcare provider(s), that determine the purposes and means of the data processing (Article 4 paragraph 7 GDPR). Third, the data processor (hereafter 'the company'): the private party or parties that deliver the m-Health infrastructure and process data in this respect (Article 4 paragraph 8 GDPR).

### Company that provides m-Health infrastructure

Before offering m-Health to patients, the HCP—as data controller—makes a clear agreement with his processor, the company that provides the appropriate infrastructure. In their agreement—called a 'data processing agreement' (DPA)—they decide on the specific purpose and nature of the data processing (Article 28 paragraph 3 GDPR). Because the processor acts on behalf of the controller, the HCP is the party that determines the content and conditions of the agreement, and the company the party that assists the controller with compliance with the obligations of the GDPR. Would a company, established outside the EU, be involved in m-Health, offered to patients in the EU, it would still be bound by the provisions of the GDPR (Article 3 paragraph 1 GDPR).

#### Onboarding of patient

In order to ensure correct identification, the patient is physically present on site when the m-Health programme is started. The patient provides consent—in this case: for a health monitoring programme—to his HCP. Consent needs to be obtained before any data collecting or processing; it should be freely given, and be based on sufficient and clear information, including the identity of all parties receiving patient data. In the Netherlands, the doctor–patient is regulated by civil law—by the 'Medical Treatment Contract Act'—although it can also be regulated by public law. An important provision of this act is the one that ensures medical confidentiality, implying that patient data may not be shared with professionals that are not involved in the patient's treatment without prior consent.

Apart from the Medical Treatment Contract Act, the GDPR requires informed consent (Article 7 GDPR), but in this case specifically for processing the patient's data. It is again the HCP who is responsible for informing the patient and asks his or her consent before any data collection or processing is carried out; consent should be freely given, and be based on sufficient and clear information, including the identity of the HCP as controller and all parties receiving patient data (Article 13 GDPR). Written consent is not required, however, as long as 'the controller (HCP) shall be able to demonstrate that the data subject has consented' (Article 7 paragraph 1 GDPR). The patient has the option to withdraw consent, after which the m-Health programme and data collection should be terminated.

#### Health data collection

Health data are collected by patients through medical devices that are connected with an application on smartphone or tablet after preferably a safe login with two-factor authentication. After performing

**Table 1** Phases of data processing and implications from data protection legislation (GDPR)

| Phase | Element | Implications from data protection legislation (GDPR) | Points of attention | HartWacht learning points |
|---|---|---|---|---|
| 0 | Onboarding of patient | ▶ The patient is identified (by being physically present).<br>▶ Informed consent is obtained on treatment and processing of health data in context of m-Health programme. | ▶ Consent for data processing is: freely given; specific; informed; and unambiguous. | ▶ Only sign up patients after a visit to the outpatient clinic in which patient is informed about HartWacht. |
| 1 | Data collection | ▶ Disclosure of relevant data stored and processed.<br>▶ Certification for data collectors. | ▶ Using a login with two-factor authentication.<br>▶ Legal position of company as data processor (and controller). | ▶ Provide patients with validated and certified mobile applications of contracted partners.<br>▶ Fully automated integration between mobile application and hospital information system. |
| 2 | Data transmission | ▶ Data controller and data processor reach agreement about processor's activities and duties (data processing agreement, DPA). | ▶ Applying highest level of encryption as described in ICT-security guidelines.<br>▶ When involving cloud services: additional security and confidentiality risks. | ▶ DPA between CCN and manufacturers of devices and applications. |
| 3 | Data storage on external servers | ▶ Data processor provides appropriate technical and organisational measures to facilitate data processing according to data protection principles (such as data minimisation) in accordance with DPA. | ▶ Storing health data on servers in countries outside EU, not providing adequate level of data protection. | ▶ Agreed with data processors to store the data in Netherlands and Ireland (EU). |
| 4 | Sharing of personal data | ▶ Data are shared in line with purpose description in DPA, unless data are aggregated and no longer considered personal data in light of GDPR. | ▶ Sharing personal data for other purposes than initial description in DPA. | ▶ Sharing of data limited to the purpose described in the DPA, such as device distribution or generation of medical data. |
| 5 | Sharing of aggregated data | ▶ Data are shared in line with purpose description in DPA, unless data are aggregated and no longer considered personal data in light of GDPR. | ▶ When using personal data for medical data research: not without consent or without meeting conditions of consent exemption. | ▶ Only data not considered personal data might be used for research purposes. |
| 6 | Data storage by healthcare provider | ▶ Hospital information system meets required security safeguards.<br>▶ Supervising data protection officer is appointed and a Data Privacy Impact Assessment (DPIA) is performed. | ▶ Duty to notify data breaches within 72 hours after discovery. | ▶ Making use of a hospital information system containing the appropriate ISO certifications.<br>▶ Repeating the DPIA for each structural change in HartWacht. |
| 7 | Data interpretation by healthcare provider | ▶ Designing the m-Health infrastructure for purposeful data processing (privacy by design and default). | | ▶ Limit data collection to relevant parameters: only blood pressure in the hypertension group, only EKG in the arrhythmia group. |

CCN, Cardiology Centres of the Netherlands; EKG, Electrocardiogram; EU, European Union; GDPR, General Data Protection Regulation; ISO, International Organization for Standardization.

measurements, data are (partly) stored locally on the smart devices owned by the patients.

### Health data transmission

Health data that are recorded by the patient are transferred to servers of the company that is engaged in m-Health as data processor. It is the HPC's responsibility to cooperate only with data processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject (Article 28 paragraph 1 GDPR). In order to minimise risks of incidents during the transmission of the data, both parties—the HCP and the company—are responsible to implement appropriate technical and organisational measures to secure data transmission. In general, because health data are considered highly sensitive, those measures should provide the highest level of protection. Although data encryption is explicitly mentioned as an appropriate measure (Article 32 paragraph 1 GDPR), the GDPR does not describe which encryption methods are considered adequate. In general, however, in case of processing health data, encryption methods as described in ICT-security

guidelines or standards, such as ISO (International Organization for Standardization)/ICE (Institute for Credentialing Excellence) 27001 are required (Article 43 paragraph 1 sub b GDPR). However, useful it may be to involve cloud services for data transmission (because of their increased scalability and flexibility), it obviously implies enlarged risk of infringing security and patient confidentiality. It is important that the HCP knows if the company involves cloud services (including their geographical location) in providing its services and is notified when personal data breaches occur (Article 33 GDPR).

#### Health data storage on external servers

After transfer, health data are stored on servers of the company. In its role as controller, the HCP needs to imply appropriate technical and organisational measures to ensure that only the data that are necessary for the specific purpose of the cooperation are collected and stored (data minimisation) (Article 25 paragraph 2 GDPR).

#### Sharing of personal data

Data processors (the companies that delivers the m-Health infrastructure) are required to minimise the data that are collected and limit it to what has been agreed on with the data controller (Article 28 paragraph 3 sub a GDPR). Processing of health data for purposes outside the professional healthcare domain (such as medical data research or product development or other commercial purposes) is strictly prohibited without prior consent.

#### Sharing of aggregated data

In the case of an m-Health infrastructure, aggregated and truly anonymised data do not fall within the scope of the GDPR and could be used for statistical purposes or medical data research. Data with information that can be attributed to an identifiable person is not considered anonymous but pseudonymised and therefore the GDPR does apply (Recital 26 GDPR). Pseudonymised data may only be used for these purposes after explicit informed consent[9] (Article 6 paragraph 1 sub a GDPR and Article 9 paragraph 2 sub a GDPR).

#### Data storage by data controller

The HCP as data controller is required to maintain a record of all processed data in the m-Health programme (Article 30 paragraph 1 GDPR) and use a hospital information system with adequate security safeguards. Other responsibilities include designating a data protection officer (DPO) (Article 37 GDPR) and executing data protection impact assessments (Article 35 GDPR). The tasks of the DPO are explicitly mentioned in the GDPR and include, among other things, to monitor compliance with the GDPR and cooperate with supervisory authority if necessary (Article 39 paragraph 1 GDPR). In the case of a personal data breach the healthcare institution should notify the local authority within 72 hours after discovery (Article 33 paragraph 1 GDPR).

#### Data analysis by HCP

In this phase of data processing, 'privacy by design' and 'privacy by default' are important principles (Article 25 GDPR). This means, for instance, that the m-Health programme is designed in such a way that only personal data which are necessary for each specific purpose of the processing are processed (Article 25 paragraph 2 GDPR). Recognised certification can serve as an indicator to authorities that the data controller has complied with these requirements (Article 25 GDPR).

## COMPLIANCE ISSUES WITH DATA PROTECTION LEGISLATION HEALTHCARE PROVIDERS SHOULD BE AWARE OF

As explained above, the GDPR has important consequences for the emerging field of m-Health whereas its functioning is largely dependent on the processing of health data; the presented 'roadmap' (see figure 2 and table 1) seeks to support healthcare providers who intend to set-up and implement a GDPR-compliant m-Health infrastructure. In this paragraph, we briefly discuss three issues related to complying with the GDPR.

### Applicability of the GDPR

A first issue is whether data processing or certain parts fall within the scope of the GDPR. When data are truly anonymised the latter is not the case. In that situation, data may be processed by any party for any legitimate purpose, varying from commercial purposes to medical research or statistics. But the GDPR sets the bar high on anonymisation, stating in Recital 26 GDPR that data are anonymous where it does 'not relate to an identified or an identifiable person'. Anonymisation is a technique applied to personal data in order to achieve irreversible de-identification.[13] The same recital makes very clear that personal data which is 'only' pseudonymised, should be still considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, (…) 'account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments'.

However, the line between anonymous and personal data can, in practice, be difficult to draw. Therefore, we advise to be on the safe side: in case of doubt on the

identifiability of the data, they should be considered to be personal non-anonymised data and fall within the scope of the GDPR.

### Legal position of company providing m-Health

In general, the HCP is 'data controller', and the company that delivers the m-Health structure 'data processor'. This is an important distinction because the GDPR treats the two very differently. The data controller, determining the purposes and the nature of the data processing, is the principal accountable party and carries the main responsibilities. The data processor merely performs certain activities with personal data, according to previously made contractual agreements with the data controller in a DPA, and has, therefore, as its main GDPR-responsibility, to ensure an adequate level of security, suitable to the risk of data processing (Article 32 paragraph 1 GDPR). When a device and application manufacturer simply carries out its assignment, it can be seen as a data processor. But if the company would do more with its collected patient data, for instance, process these for commercial or research purposes, it needs to be regarded also as a (second) data controller according to the GDPR, implying that all corresponding duties for controllers apply. In the latter situation, the company's responsibilities under the GDPR are much more extensive than in the first situation.

### Involving cloud services

Because of their technical possibilities and flexibility, it may be profitable for data controllers and processors to involve cloud services in providing m-Health, for instance, to obtain on-demand availability of data storage via the internet—the latter at relatively low costs and minimal maintenance activities. When a cloud service company is involved, this party would, similar to the device company, qualify as a data processor. How attractive this may be, the controller's and processor's joint responsibilities on appropriate security measures and safeguards should be assessed even more carefully in this setting. We aim especially at increased privacy and confidentiality risks, caused by, for instances, strict legislation on national security and terrorism in countries outside Europe, such as China and the USA. From privacy perspective, a cloud service based within the EU is preferable. An overview of the current involvement of cloud services in general healthcare does not exist, but a survey shows an adoption of 35% by HCP in the USA in 2016 of which 93% does not meet the standard of data security.[14]

## FINAL REMARKS

Innovative ways of healthcare delivery, such as medicine by mobile and wearable devices, seem very promising in improving quality of care at lower costs. Therefore, we should encourage them, but not without paying proper attention to the principles and requirements of data protection legislation. The GDPR was enforced in May 2018 to ensure data protection of all EU citizens. Just like in medical data research, there has to be a fair balance between data protection and data processing for legitimate purposes. In medical research, this is progression of scientific knowledge, in m-Health this is innovation that could lead to better quality of care for patients at lower costs.[15] The challenges and pitfalls we provide in this manuscript hopefully help healthcare providers starting m-Health initiatives to comply with its most important provisions. The m-Health specific Privacy Code of Conduct (2015), established by the European Commission[16] but yet to be approved,[17] also gives practical guidance. The most important responsibility for healthcare providers is to inform patients on data processing and to obtain their explicit consent. Only by complying with these and other GDPR-provisions, m-Health can live up to its promises in the near future.

**Author affiliations**
[1]Cardiology, Amsterdam UMC - Locatie AMC, Amsterdam, The Netherlands
[2]Cardiology, Dijklander Ziekenhuis, Hoorn, North-Holland, The Netherlands
[3]Cardiology, Cardiologie Centra Nederland, Amsterdam, The Netherlands
[4]Medical Physics/Cardiology, LUMC, Leiden, The Netherlands
[5]Internal Medicine, Amsterdam UMC - Locatie AMC, Amsterdam, The Netherlands
[6]Cardiology, Onze Lieve Vrouwe Gasthuis, Amsterdam, The Netherlands
[7]Cardiothoracic Surgery, Amsterdam UMC - Locatie AMC, Amsterdam, The Netherlands
[8]Health Law, Amsterdam UMC - Locatie AMC, Amsterdam, The Netherlands

**Contributors** EW, SB, MCP, MMW: Planning writing. GAS, ETvdV, IIT, BS, MCCdW, BJHvdB: reviewing. LB: Writing. BAJMdM: Supervision.

**Funding** The authors have not declared a specific grant for this research from any funding agency in the public, commercial or not-for-profit sectors.

**Competing interests** None declared.

**Patient consent for publication** Not required.

**Provenance and peer review** Not commissioned; externally peer reviewed.

**Data availability statement** No data are available.



ORCID iD
Eric Wierda http://orcid.org/0000-0002-9998-5035

## REFERENCES

1 European Commision. *Green paper on mobile health*. Brussels, 2014.
2 World Health Organisation, eHealth. *eHealth resolutions to the 58th meeting of the World Health Assembly*, 2004: 121–3.
3 Cowie MR, Bax J, Bruining N, *et al*. e-Health: a position statement of the European Society of cardiology. *Eur Heart J* 2016;37:63–6.
4 Kaewkannate K, Kim S. A comparison of wearable fitness devices. *BMC Public Health* 2016;16:433.

5 Pevnick JM, Birkeland K, Zimmer R, *et al*. Wearable technology for cardiology: an update and framework for the future. *Trends Cardiovasc Med* 2018;28:144–50.
6 Maric B, Kaan A, Ignaszewski A, *et al*. A systematic review of telemonitoring technologies in heart failure. *Eur J Heart Fail* 2009;11:506–17.
7 Quinn P, Habbig A-K, Mantovani E, *et al*. The data protection and medical device frameworks - obstacles to the deployment of mHealth across Europe? *Eur J Health Law* 2013;20:185–204.
8 European Union. Regulation 2016/679, 2016. Available: http://eur-lex.europa.eu/pri/en/oj/dat/2003/l_285/l_28520031101en00330037.pdf
9 Wierda E, Eindhoven DC, Schalij MJ, *et al*. Privacy of patient data in quality-of-care registries in cardiology and cardiothoracic surgery: the impact of the new general data protection regulation EU-law. *Eur Heart J Qual Care Clin Outcomes* 2018;4:239–45.
10 McCall B. What does the GDPR mean for the medical community? *Lancet* 2018;391:1249–50.
11 ANNEX - health data in apps and devices.
12 Botrugno C. Telemedicine in daily practice: addressing legal challenges while waiting for an EU regulatory framework. *Health Policy Technol* 2018;7:131–6.
13 Opinion, 05/2014 on Anonymisation techniques, adopted 10 April 2014, 0829/14/EN, 7.
14 Cloud adoption and risk report 2019. Available: https://cloudsecurity.mcafee.com/cloud/en-us/forms/white-papers/wp-cloud-adoption-risk-report-2019-banner-cloud-mfe.html?Source=Website&LSource=Website&_ga=2.255771656.1080209401.1565257284-1045511020.1565257284
15 Ploem MC, Essink-Bot ML, Stronks K. Proposed EU data protection regulation is a threat to medical research. *BMJ* 2013;346:f3534.
16 European Commission. Privacy code of conduct on mobile health apps, 2018. Available: https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps
17 Graux H. *Article 29 data protection Working Party*. Brussels, 2018.