


Remote monitoring of cardiac implanted electronic devices: legal requirements and ethical principles - ESC Regulatory Affairs Committee/EHRA joint task force report

Jens Cosedis Nielsen ^{1*}, Josef Kautzner², Ruben Casado-Arroyo³, Haran Burri⁴, Stefaan Callens⁵, Martin R. Cowie⁶, Kenneth Dickstein⁷, Inga Drossart⁸, Ginger Geneste⁹, Zekeriya Erkin⁹, Fabien Hyafil¹⁰, Alexander Kraus¹¹, Valentina Kutyla¹², Eduard Marin^{13,14}, Christian Schulze¹⁵, David Slotwiner¹⁶, Kenneth Stein¹⁷, Stefano Zano¹⁸, Hein Heidbuchel¹⁹, and Alan G. Fraser^{20,21}

¹Department of Cardiology, Aarhus University Hospital, Palle Juul-Jensens Boulevard 99, DK-8200 Aarhus N, Denmark; ²Institute for Clinical and Experimental Medicine, Prague and Palacky University Medical School, Olomouc, Czech Republic; ³Department of Cardiology, Erasme University Hospital, Université Libre de Bruxelles, Brussels, Belgium; ⁴Cardiac Pacing Unit, Cardiology Service, University Hospital of Geneva, Geneva, Switzerland; ⁵Centre for Biomedical Ethics and Law, KU Leuven, Leuven, Belgium; ⁶Imperial College London (Royal Brompton Hospital) & National Heart and Lung Institute, Dovehouse Street, London SW3 6LY, UK; ⁷University of Bergen, Stavanger University Hospital, Stavanger, Norway; ⁸ESC Patient Forum member, Brussels, Belgium; ⁹Cyber Security Group, Delft University of Technology, Delft, The Netherlands; ¹⁰Département Médico-Universitaire DREAM, Bichat University Hospital, APHP.7, Inserm 1148, Université de Paris, Paris, France; ¹¹BIOTRONIK SE & Co. KG, Berlin, Germany; ¹²University of Rochester Medical Center, Clinical Cardiovascular Research Center, Rochester, NY, USA; ¹³School of Computer Science, University of Birmingham, Birmingham, UK; ¹⁴Telefonica Research, Spain; ¹⁵Division of Cardiology, Angiology, Pneumology and Intensive Medical Care, Department of Internal Medicine I, University Hospital Jena, Friedrich-Schiller-University Jena, Am Klinikum 1, Jena, Germany; ¹⁶Division of Cardiology, New York Presbyterian Queens and School of Health Policy and Research, Weill Cornell Medical College, New York, NY, USA; ¹⁷Boston Scientific, Arden Hills, MN, USA; ¹⁸Dipartimento di Elettronica, Informazione e Bioingegneria, Politecnico di Milano, Milan, Italy; ¹⁹Department of Cardiology, University Hospital Antwerp, University of Antwerp, Antwerp, Belgium; ²⁰School of Medicine, Cardiff University, Cardiff, UK; and ²¹Department of Cardiovascular Sciences, Katholieke Universiteit Leuven, Leuven, Belgium

Received 15 April 2020; editorial decision 21 May 2020; accepted after revision 25 May 2020

Abstract

The European Union (EU) General Data Protection Regulation (GDPR) imposes legal responsibilities concerning the collection and processing of personal information from individuals who live in the EU. It has particular implications for the remote monitoring of cardiac implantable electronic devices (CIEDs). This report from a joint Task Force of the European Heart Rhythm Association and the Regulatory Affairs Committee of the European Society of Cardiology (ESC) recommends a common legal interpretation of the GDPR. Manufacturers and hospitals should be designated as joint controllers of the data collected by remote monitoring (depending upon the system architecture) and they should have a mutual contract in place that defines their respective roles; a generic template is proposed. Alternatively, they may be two independent controllers. Self-employed cardiologists also are data controllers. Third-party providers of monitoring platforms may act as data processors. Manufacturers should always collect and process the minimum amount of identifiable data necessary, and wherever feasible have access only to pseudonymized data. Cybersecurity vulnerabilities have been reported concerning the security of transmission of data between a patient's device and the transceiver, so manufacturers should use secure communication protocols. Patients need to be informed how their remotely monitored data will be handled and used, and their informed consent should be sought before their device is implanted. Review of consent forms in current use revealed great variability in length and content, and sometimes very technical language; therefore, a standard information sheet and generic consent form are proposed. Cardiologists who care for patients with CIEDs that are remotely monitored should be aware of these issues.

* Corresponding author. Tel: +45 4013 5295. E-mail address: jenniels@rm.dk

Published on behalf of the European Society of Cardiology. All rights reserved. © The Author(s) 2020. For permissions, please email: journals.permissions@oup.com.

Keywords

Remote monitoring • Cardiac implantable electronic device • General Data Protection Regulation • Informed consent • EHRA • ESC Regulatory Affairs Committee • Cybersecurity • Informed consent form • Data controller • Data processor • Joint data controller

Introduction

The General Data Protection Regulation (GDPR) that has been implemented in the European Union (EU) since 2018 provides a common legal framework in all member states.¹ It governs how personal information can be collected and must be managed, and it provides a clear structure of accountability in the event that data security becomes compromised or if an individual has questions or concerns or chooses no longer to share their personal data.

Technological advances have enabled increasing numbers of patients to benefit from remote monitoring (RM) of their medical devices, which has led to vast amounts of personal health data circulating via interconnected systems. This is especially true with respect to cardiac implantable electronic devices (CIEDs) such as implantable cardioverter-defibrillators (ICDs), pacemakers, cardiac resynchronization therapy devices, and loop recorders, for which RM is now a standard procedure. Individuals have the right to control who has access to their personal data and how it is used, so patients are asked to sign consent forms that allow manufacturers to have remote access to their device data and sometimes also to share these data with third parties.

In 2018, a Task Force was convened between the Regulatory Affairs Committee of the European Society of Cardiology (ESC) and the European Heart Rhythm Association (EHRA), to consider the remote monitoring of CIEDs. Industry and Heart Rhythm Society (HRS) representatives were part of the task force. How are data encrypted and transmitted, where does identifiable information go, who handles it, and with whom is it shared? Who is responsible for the data and its processing, and how should informed consent be obtained? Are clinicians subject to any specific liability? Are standards applied consistently by healthcare providers and manufacturers? This report addresses these questions and recommends standard procedures that hospitals and physicians can adopt in order to meet their obligations under the GDPR.

Remote interrogation and monitoring of cardiac implantable electronic devices

Remote CIED management was pioneered by Biotronik (Berlin, Germany) which introduced its Home Monitoring[®] system in 2001. All manufacturers currently propose remote device management,² which involves the seamless transmission of data over a network from the patient's location via a central database to a hospital or physician's office. Optionally, third-party providers may process the data for triage of alerts or centralization of transmissions from different manufacturers on a common platform. The data include the functional status of the device and device-monitored patient variables.

Remote follow-up which replaces scheduled in-office visits can be distinguished from RM involving automatic unscheduled transmission of pre-specified alert events such as arrhythmias or abnormal lead impedance, and from patient-initiated transmissions or unscheduled follow-ups initiated manually by the patient as a result of a real or perceived clinical event.³ The overriding goal is to improve the prognosis of patients through early detection of events and proactive corrections.

International standards that are relevant for RM are reviewed in [Supplementary material online, Appendix S1](#). Remote monitoring provides a platform for storing and analysing data, with a wealth of information that can be used both for clinical management, research⁴⁻⁶ and for tracking the technical performance of CIEDs. Manufacturers use data obtained by RM to guide iterative developments of their medical devices and to increase the efficiency and reduce the costs of clinical investigations. For example, RM data obtained from subcutaneous ICDs led to a new algorithm that reduced inappropriate shocks that had been triggered by over-sensing, by 70%.⁷ Remote monitoring also provides data that manufacturers must collect to establish the long-term safety and performance of their devices.

The clinical benefits of RM have been reviewed elsewhere.⁸⁻¹⁰ Remote monitoring is a Class IIa (level of evidence A) recommendation according to the 2013 EHRA/ESC guidelines, to provide earlier detection of clinical problems and technical issues.¹¹ A more recent Heart Rhythm Society expert consensus states that RM should be offered to all CIED patients as part of standard follow-up (Class I, level of evidence A).¹² A health technology assessment concluded that RM of CIEDs is cost-effective for surveillance and control of the device.⁹ The TRUST trial demonstrated that RM is safe, since it was not associated with any increase in morbidity,¹³ but further research is needed to determine the impact of RM on clinical outcomes and prognosis. Despite these recommendations, only a minority of CIED patients in Europe are placed on remote device management, mainly due to lack of reimbursement.¹⁴ This implies that RM should be funded as an integral component of continuous care. The need for guidance on legal aspects of RM has been recognized for some years.¹⁵

Regulations relevant to the remote monitoring of cardiac implantable electronic devices in Europe**European Union General Data Protection Regulation**

The GDPR was approved by the European Parliament and the Council of the EU in 2016¹ and applied after a transition period from 25 May 2018. It replaced the EU Data Protection Directive from

1995 which was recognized as being out of date due to technological advances. The main objective of the GDPR is to ensure 'the protection of natural persons with regard to the processing of personal data and on the free movement of such data'. The purpose of collecting and retaining data should be limited and specified, and processing of personal data should be undertaken only with specific consent (Article 6.4). The definition of personal data in the GDPR includes all data pertaining to the health status of a data subject, so it encompasses data collected by CIEDs and transferred by RM systems.

A key principle enacted by this legislation is that individuals and organizations collecting and retaining data should be accountable. Specific legal responsibilities are described for the 'data controller', defined as the person or body which determines the purposes and means of processing personal data, and the 'data processor', defined as the person or body which processes personal data on behalf of the controller and in accordance with any limitations established by the controller (Article 4). The GDPR states that there may be more than one controller, and it reconfirms the concept of joint controllers where two or more controllers together determine the purposes and means of processing data. In case of joint controllers (Article 26) or in case of a controller and a processor (Article 28) arrangements must formally determine their respective responsibilities with regard to compliance with the GDPR, as in case of any breach both parties will need to justify their accountability. The GDPR does not address data sharing between independent controllers, and in most cases, such relationships are set out in an agreement. Significant financial penalties can be imposed on data controllers or processors if they fail to meet their responsibilities.

Use of personal data

Individuals are granted the right to obtain information from the data controller about the nature and use of the data stored, and they have the right of access to their own data. With certain exemptions (such as when the security of the state must be protected) they have the right to be forgotten and to have their data erased from a particular database (Article 17). Data subjects also in general have the right to 'data portability' which means that they can receive their personal data in a 'structured, commonly used and machine-readable format', thereby allowing them to transmit those data to another controller without hindrance from the controller to which the personal data have been provided (Article 20).

In one of the preambles to the GDPR (Recital 33), it is recognized that it is often impossible at the time that personal data are collected to identify all the purposes for which those data will be processed for scientific research. Thus, in such instances, subjects are allowed to give their consent to certain areas of scientific research when this is in keeping with recognized ethical standards.

Article 5 states that further processing of personal data for scientific or statistical purposes is possible. Article 6.1.c states that processing is lawful if it is necessary for compliance with a legal obligation to which the controller is subject. According to the European Data Protection Board (opinion 3/2019, recitals 12 and 13),¹⁶ this may provide a legal basis for the processing of personal data in the context of safety reporting; in the context of an inspection by a national competent authority; for the retention of clinical trial data in accordance with archiving obligations set up by the EU Clinical Trials Regulation;¹⁷ or for a sponsor and/or investigator to comply with

relevant national laws. According to Article 6.e, processing is lawful if it is necessary for the performance of a task carried out in the public interest.

The principles of Article 6 relate to personal data in general. With regard to specific categories, Article 9.2.g states that health data can be processed if necessary for reasons of substantial public interest. Health data can also be processed for scientific or historical research or statistical purposes, in accordance with Article 89.1 based on EU or Member State law (Article 9.2.j). So, although the processing of personal data concerning health is in principle prohibited (Article 9.1), several exceptions are provided. Article 9.2.a allows the processing of health data on the basis of explicit consent of the person concerned. Processing is also allowed if it is necessary for the provision of health care or treatment, or for management of health or social care systems and services, on the basis of Union or Member State law or pursuant to contract with a health professional. Finally, health data can also be processed for reasons of public health such as ensuring 'high standards of quality and safety of medical devices, on the basis of EU or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy' (Article 9.2.i).

It follows from all the above that explicit consent is not always required for processing health data, such as when clinical staff review patients' health records or other medical data for making a diagnosis or treatment plan. This would include outputs from RM.

Legal advice

For this review, the Task Force commissioned and obtained expert legal advice on the specific interpretation of the requirements of the GDPR in the context of RM of implanted electronic medical devices.¹⁸

Any company that determines the means and purposes of collecting personal data is considered to be operating as a data controller (Article 29 Working Party, page 21).¹⁶ For manufacturers which set up systems for CIEDs, 'means' applies not only to the technology used to collect data but also to the selection and the format of data required for efficient RM. The controller is responsible for providing access to the personal data collected and it should offer the possibility to delete them (Article 29 Working Party, page 15).¹⁶

Physicians, healthcare professionals and hospitals may have dual or independent roles (*Figure 1*). Regarding RM of CIEDs of their patients, the healthcare facility or hospital should always be considered a data controller. Sometimes this will be together with the healthcare professional if the healthcare professional is a self-employed physician who works in the healthcare facility and acts as a controller; otherwise, a hospital takes legal responsibility as controller for staff whom it employs. The healthcare facility or hospital has to make a proper contractual agreement with the manufacturer (*Figure 1*), taking into account the specific rules that apply when transferring personal data outside the EU.¹⁹

The legal advice recommended that the relationship between the healthcare facility and the manufacturer for the management and protection of data generated by RM of CIEDs should be as joint data controllers.¹⁸ Formal and transparent agreement on the responsibilities and duties of each party in relation to the collection of individual data (Article 26) should include details on how individuals can have access

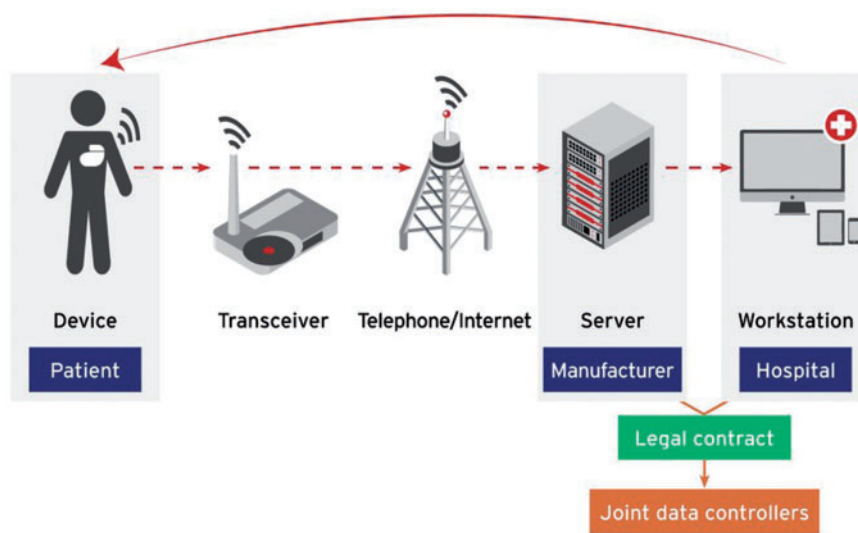
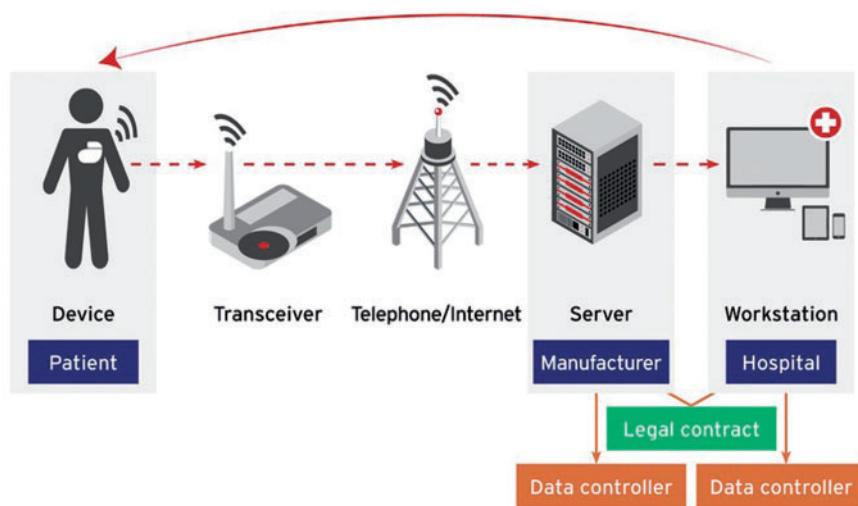
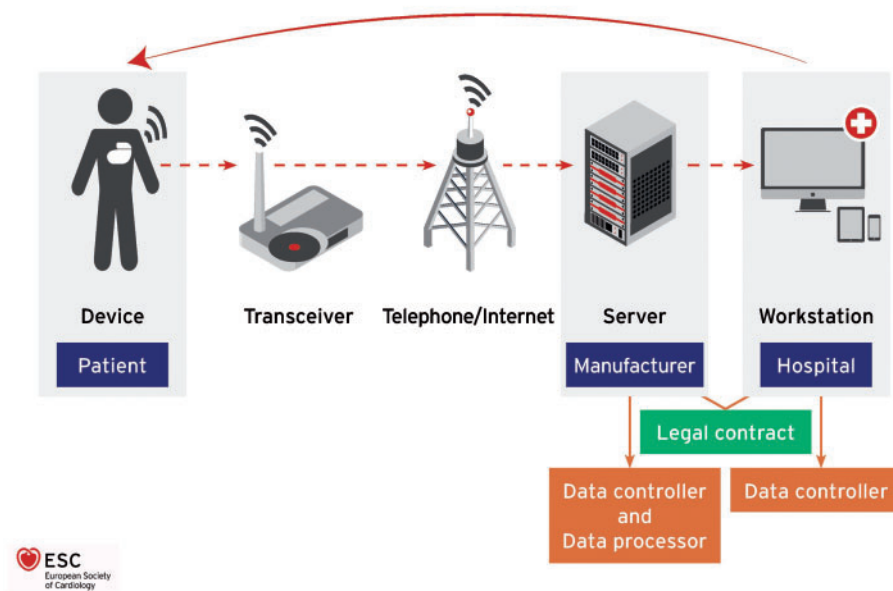
Option 1: Joint controllers**Option 2: Two controllers**

Figure 1 The figure illustrates the data flow in RM of CIEDs. Data are automatically transferred via a transceiver and the mobile telephone network to secure servers that are specific for each manufacturer. Data are filtered and displayed for the hospital on manufacturer-specific webpages, and the hospital can contact to the patient when needed (upper arrow). Legally, the *data controller* is defined as the person or body which determines the purposes and means of processing personal data, and the *data processor* as the person or body which processes personal data on behalf of the controller and in accordance with any limitations established by the controller. Both the hospital and manufacturers are typically considered data controllers, while third-party providers are considered data processors (orange boxes). For all controller–controller and controller–processor relationships, a formal and transparent contract (green boxes) describing the responsibilities and duties of each party in relation to the collection and handling of individual data must be made. Options 1–4 describe the different controller–controller and controller–processor relationships. Option 3 illustrates the situation where the manufacturer acts as data processor to the hospital (which in that relationship is acting as data controller), but where it is also considered as data controller when analysing data for purposes other than those set by the hospital. CIEDs, cardiac implantable electronic devices; RM, remote monitoring.

Option 3: Manufacturer as controller and processor



Option 4: Manufacturer and/or Hospital using Another Party as data processor

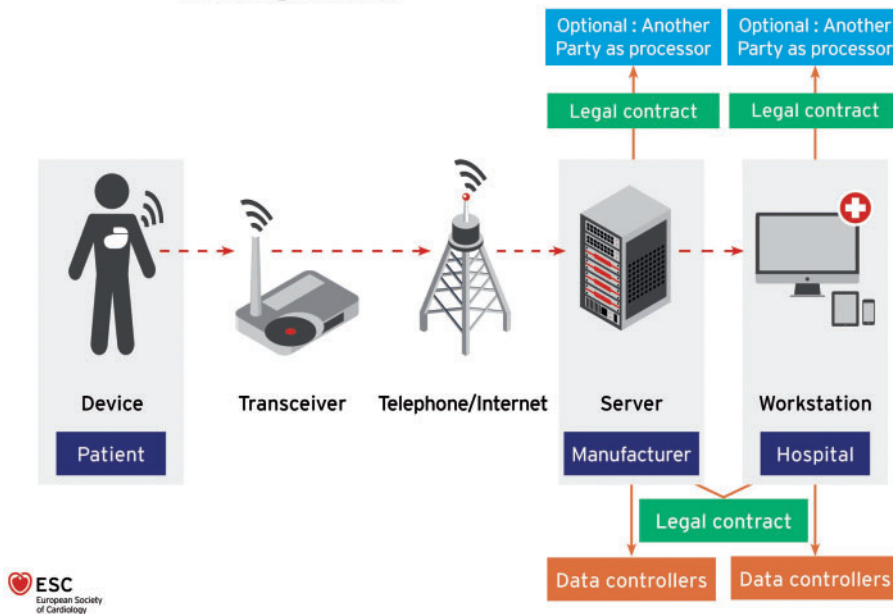


Figure 1 Continued

to their personal data or modify them or request for their deletion (Articles 13 and 14).¹ The recommended relationship of a third-party provider of telemonitoring services with a hospital or manufacturer (as controller) is as a data processor.

Manufacturers of CIEDs are also governed by relevant provisions of the EU Medical Device Regulation (MDR)²⁰ as summarized in [Supplementary material online, Appendix S2](#). Pre-market investigation

of a CIED should include clinical evaluation of the hardware and software used for RM. The GDPR states that any software must protect privacy by design and by default (Article 25) and that a risk analysis concerning data protection must be conducted for each project. The MDR requires manufacturers to conduct post-market surveillance, which for CIEDs includes collecting and analysing the technical performance data provided by RM of their devices. That provision

may appear incompatible with the right given to individuals by the GDPR to require their personal information to be removed from a database, but no problem would arise if manufacturers stored only anonymized or pseudonymized data (see Article 4.5 of the GDPR). Questions requiring legal guidance have been reviewed in more detail elsewhere.²¹

Current status of remote monitoring in Europe

Views of patients

The literature on patient-reported experiences of RM is scarce. In 2012 it was reported that 95% of 385 Scandinavian patients with ICDs were 'content' or 'very content' with RM.²² Benefits reported anecdotally include having felt safer and/or better looked after because continuous monitoring gave some 'peace of mind', and being able to transmit data when feeling unwell or having experienced an event. The REMOTE-CIED study of 300 European heart failure patients with ICDs also found very high rates of satisfaction.²³ Patients living in remote areas especially appreciated fewer follow-up visits to the hospital or their doctor's office. Nonetheless, 53% of patients experienced issues such as failure to transmit data, and 19% of the 221 patients who reported their follow-up preferences stated that they wished to remain under review in a hospital clinic.²³

In response to a general consultation about mobile health in 2015, 46% of the 211 replies to a European Commission survey considered that strong privacy and security tools (such as data encryption and authentication mechanisms) are needed to build users' trust. Half of the respondents called for a strengthened enforcement of data protection and rules applicable to mobile health (mHealth) devices.²⁴ Another consultation showed very strong support for members of the public to be fully informed about how their data are used.²⁵ Nonetheless, reports by manufacturers, third parties involved in RM, or physicians have not reported many patients expressing concerns with regard to data protection and cybersecurity. These topics also seem not to come up regularly in patients' support groups, unless there is media coverage about possible hacking of devices.

Consent for RM is often obtained from patients after their CIED has been implanted and before they are discharged from hospital, when they may still be uncomfortable or even in pain and are probably focused on going home and recovering. In those circumstances, patients may sign the consent form quickly without having read or thoroughly understood the information provided. The optimal timing for obtaining this consent needs more study but based upon advice that was received from patients and agreement among the Task Force members, it is probably before rather than after implantation. In cases where this is not possible, such as when a device is implanted in an acute situation, clinics should set up a routine protocol for explaining RM and obtaining informed consent post-operatively during a physical visit. Information needs to be provided in language and in a format that is easy for patients to understand.

Knowledge of doctors—results of survey

In a survey conducted by EHRA in 2014, only 9% of physicians reported being aware of legal issues related to the RM of CIEDs.²⁶

This Task Force conducted a further on-line survey concerning knowledge about RM of CIEDs, during 2019. We received 320 responses from cardiac electrophysiologists (47%), general cardiologists (29%), heart failure physicians (8%), and technicians, nurses, and fellows (16%), coming from 27 ESC member countries. Low-volume (<100 CIED implants/year), mid-volume (100–500/year), and high-volume centres (>500/year) were represented by 24%, 49%, and 27% of replies, respectively.

In this new survey, 49% of respondents answered that they were aware of the GDPR, without necessarily knowing its implications with respect to RM of CIEDs. According to the specific definitions in the GDPR, the majority (58%) identified themselves as data 'controllers', while 42% identified themselves as 'processors'. About half of the respondents (44%) considered the GDPR as having moderately or significantly impacted their RM practice; as particular issues, they identified logistics (52%) and increased demands on their time (50%). Only 4% cited its legal impact.

Cybersecurity issues were acknowledged by 61% of survey participants, with 38% undertaking specific steps to address these concerns at their institution, including the use of firewalls (61%), encryption (39%), new local policies (38%), legal advice (36%), two-factor authentication (33%), and/or revision of their consent form (25%). Regarding the patient's perspective, 92% of the respondents reported that their patients never or rarely voice concerns regarding the safety of their data when having their CIED remotely monitored or ask about access to their remotely collected CIED data.

These findings highlight the need for this consensus document to provide a common interpretation of the GDPR.

Viewpoint of manufacturers and third-party providers

A questionnaire relating to GDPR and cybersecurity was sent to all manufacturers of CIEDs available on the European market, as well as to some third-party providers. All replied with information that was used to construct *Tables 1 and 2*. The data showed heterogeneity in the interpretation and implementation of measures relating to GDPR, and manufacturers indicated that hospitals specify diverging requirements for protecting data.

All five companies defined the healthcare institutions as data controllers (*Table 1*). Most manufacturers, who are based outside the EU, informed us that they consider themselves only to be data processors. Two companies reported that they considered themselves also to be data controllers; another included physicians as controllers. These opinions diverge from the general guidance prepared for the European Commission and from our legal advice.^{16,18}

All manufacturers of CIEDs report that they apply measures to ensure cybersecurity when transferring data from the transceiver to the server and hospital. They monitor security incidents continuously and employ methods to defend against denial of service attacks. Physical security and other environmental controls such as badges and cameras also serve to protect the RM servers. Independent intrusion tests and audits on the adequacy and effectiveness of these measures are obtained and used to adapt security systems when required.

Third-party providers of monitoring and reporting systems which were contacted for our survey, collect RM data from different

Table 1 Survey of manufacturers of CIEDs concerning GDPR

Question	Abbott	Biotronik	Boston Scientific	Medtronic	Microport
Employee access to PPD How is access to PPD controlled internally?	Access only to employees who need to perform their job, in accordance with applicable law. Appropriate technical and organizational measures.	Access to PPD is controlled by an authorization concept. Only employees who need the access according to the 'need to know' principle have access to PPD. There are technical and organizational measures in place to control the access.	Two-factor authentication. Role-based access control. Security training and procedures.	Access for those who need it for their jobs under the principle of minimum necessary. Control measures are in place to prevent accidental or unlawful destruction, loss, alteration, unauthorized disclosure, and all other unlawful forms of processing.	No-one is accessing PPD except the helpdesk agents qualified to support the patient in the shipment and installation of the home monitor. Helpdesk can only access data in read-only mode.
Do employees who have access to PPD have to undergo testing of knowledge or certification regarding GDPR?	Yes, employees are provided training on GDPR and other privacy and data protection laws.	There are regular data protection training courses and employees are bound to data secrecy.	Yes, employees train to data protection requirements in general and to GDPR specifically.	Yes, mandatory internal training and knowledge testing on general GDPR policies and procedures. Additionally, there is specific training on the recently updated CareLink Network Agreement.	Helpdesk agents undertake testing on remote monitoring before accessing the system. Training sessions including knowledge testing is launched.
Regulatory aspects Does your company consider hardware serial numbers to be PPD?	Yes	Yes	Yes	Yes	Yes, where it is possible to make the link directly or indirectly with the data subject or to deduce information about the data subject or by inference.
In which country(ies) is (are) the server(s) that store(s) the PPD from your European-based RMS located?	USA	Europe	Ireland and USA	The Netherlands	France
Who owns the PPD collected from your European-based RMS?	Concept of ownership of personal data does not exist in Europe.	The patient	Legal ownership may vary by country based on jurisprudence—PPD generally belongs to the data subject.	Concept of ownership of personal data does not exist in Europe.	Data controller (i.e. HCP)
Who do you consider to be the data controller for your RMS?	<input type="checkbox"/> Physician <input checked="" type="checkbox"/> Healthcare institution <input checked="" type="checkbox"/> Your company	<input type="checkbox"/> Physician <input checked="" type="checkbox"/> Healthcare institution <input type="checkbox"/> Your company	<input type="checkbox"/> Physician <input checked="" type="checkbox"/> Healthcare institution <input checked="" type="checkbox"/> Your company	<input type="checkbox"/> Physician <input checked="" type="checkbox"/> Healthcare institution <input type="checkbox"/> Your company	<input checked="" type="checkbox"/> Physician <input checked="" type="checkbox"/> Healthcare institution <input type="checkbox"/> Your company

Continued

Table 1 Continued

Question	Abbott	Biotronik	Boston Scientific	Medtronic	Microport
Does your company engage with third parties who transmit, use, store, or have access to the PPD of your RMS?	Yes. Local affiliated companies where required to provide customer support, and other affiliated companies for technical support.	Yes Subsidiaries for access to certain data for customer support and additional services.	Yes IT support (troubleshooting, technical interventions, maintenance)	Yes FocusOn service, when contracted with the HCP	No
Does your company ask patients to sign an informed consent, allowing your company to collect PPD coming from your RMS?	Yes	No This is the responsibility of the controller.	Yes	No It is the responsibility of the clinic or hospital to collect informed consent from patients.	No Microport provides the HCP with a template of a patient consent form.
Is the geolocation of the patient collected and stored by your company?	No	No	No	No	No
Impact of GDPR					
How many patients have contacted your company regarding issues related to GDPR?	Nominal	None	< 10 patients	Medtronic is only a data processor. Medtronic would typically request patients to contact their medical centre.	None
How has GDPR impacted the functioning of your RMS?	Mildly	Mildly	Moderately Tracking of patient consent. Renewal of data processing agreements with hospitals and updating consent forms.	Mildly	Mildly Documentation of data processing (in the Register of Processing Activity). Gap analysis of the existing measures in place Update of information notice. Training sessions. None
Please grade how GDPR has impacted product performance reporting	None	Moderately	None	Moderately	None
Please grade how GDPR has impacted your business analytics	Mildly	Moderately	None	Mildly	None
Please grade how GDPR has impacted your scientific research	Mildly	Moderately	Moderately	Mildly	None
Please grade how GDPR has impacted the daily functioning of your company	Mildly	Moderately	Moderately	Mildly	None

GDPR, General Data Protection Regulation; HCP, healthcare provider; PPD, private patient data; RMS, remote monitoring system.

Table 2 Survey of third-party providers of remote monitoring of CIEDs

Question	
Employee access to PPD	
How is access to PPD controlled internally?	<p><i>Proprietary server</i> (3):</p> <ul style="list-style-type: none"> • Process to set up users, 24/7 audit and monitoring • For every new access to the PPD a form must be filled and an approval by the executive management must be done, with traceability of access and limited time/scope. • Access is only granted to authorized people. PPD is stored in secure locations requiring specific authorizations. <p><i>VPN service</i> (2):</p> <ul style="list-style-type: none"> • All data are stored on the HCP's server, who has the responsibility to give the company and employees access to their network and information. The only contact with PPD data could be during service or maintenance tasks performed onsite or via remote login to the server of the HCP.
Do employees who have access to PPD have to undergo testing of knowledge/certification regarding GDPR?	<ul style="list-style-type: none"> • Training only (2) • Testing (3) • They also sign an IT charter/commitment (1)
Cybersecurity	
How is access to PPD that is stored on servers controlled?	<ul style="list-style-type: none"> • VPN of customer's server (2) • VPN of company's cloud-based server (1) • Company server with 24/7 audit and monitoring, SOC2 compliant (1) • VPN of customer's server OR cloud-based company server (1)
Please check off which measures are in place to <i>protect</i> your remote monitoring system from unwillingly disclosing PPD	<p>Encryption (3)</p> <p>Two-step authentication (2, under development 1)</p> <p>Firewalls (3)</p> <p>Load balancers (2)</p> <p>DDoS detection (3, and according to Microsoft Azure security measures 1)</p> <p>Other: vulnerability tests (1)</p> <p>Not applicable (customer server): 2</p>
Have you ever experienced cyberattacks (and approximately how many times)?	<ul style="list-style-type: none"> • No (3) • No significant attack (except thousands countered DDoS common on cloud-based systems) (1) • Not applicable (1)
Has the cybersecurity of your European-based remote monitoring system ever been breached?	<p>No (4)</p> <p>Not applicable; It is a customer responsibility</p>
Regulatory aspects	
Does your company consider <i>hardware serial numbers</i> to be PPD?	<p>Yes (2)</p> <p>No (2)</p> <p>Not applicable; It is a customer (healthcare institution/hospital) responsibility</p>
In which <i>country(ies)</i> is (are) the server(s) that store(s) the PPD from your European-based remote monitoring systems located?	<p>Not applicable (2)</p> <p>France (2)</p> <p>UK for UK-based customers (1)</p> <p>AWS cloud in Frankfurt, Germany (1)</p> <p>Remote support PC to access the HCP server are located in Germany (1)</p>
Who <i>owns</i> the PPD collected from your European-based remote monitoring systems?	<p>The PPD collected is the patients' property but physicians using the platform are considered the data controller.</p> <p>The Hospital</p>
Who does your company consider to be the <i>data controller</i> for the PPD collected from your remote monitoring system?	<p>Physician only (1)</p> <p>Physician + Healthcare institution (1)</p> <p>Healthcare institution (1)</p> <p>Not applicable; It is a customer (healthcare institution/ hospital) responsibility (2)</p>
Does your company ask <i>patients</i> to sign an <i>informed consent</i> , allowing your company to collect PPD coming from your remote	<p>Yes (1)</p> <p>No (3): it is the clinic or hospital's responsibility to collect informed consent from patients</p> <p>Not yet but being processed (1)</p>

Continued

Table 2 Continued

Question	
monitoring service? If yes, could you please provide it to us?	
Is the <i>geolocation of the patient</i> collected and stored by your company?	Yes (1) No (4)
Impact of GDPR	
To your knowledge, how many patients have contacted your company regarding issues related to GDPR?	None (5)
Please grade how GDPR has impacted the <i>functioning of your remote monitoring platform</i> . How?	None (2) Moderately (3). Extra measures/functionalities had to be developed to follow GDPR regulations
Please grade how GDPR has impacted your <i>business analytics</i> . How?	None (2) Mildly (1) Moderately (2)
Please rate how GDPR has impacted the <i>daily functioning of your company</i> .	None (1) Mildly (1) Moderately (2). New policies and procedures have been developed for GDPR. This has also impacted internal IT. Significantly (0) Extremely (1)

Numbers of replies are shown in brackets.

DDoS, distributed denial of service; GDPR, General Data Protection Regulation; HCP, healthcare provider; IT, information technology; PC, personal computer; PPD, private patient data; SOC2, Service Organization Control 2; SSL, Secure Sockets Layer; VPN, virtual private network.

manufacturers and process it to triage alerts. Five companies provided replies to our questionnaire (Fleischhacker[®], Focuson[®], Fysicon[®], Implicity[®], and Lindacare[®]). Their systems either employ their own servers, or they function entirely on the host's server, accessed through a virtual private network connection, or they are cloud-based. Similar to the CIED manufacturers, there is considerable heterogeneity in results of the survey (Table 2). All third-party providers consider healthcare institutions or/and physicians as data controllers (and so by default, themselves as data processors). Reported cybersecurity measures are comparable to those of CIED manufacturers.

Review of consent forms

The GDPR states that any person who allows their individual data to be shared (the 'data subject') should receive fair and intelligible information regarding the kind of individual data shared, and also the names of the recipients (Article 13.1.e). In Europe, it is common practice in most institutions to obtain informed consent for RM using forms created and provided by the manufacturers, rather than forms made by each institution. Consent should be obtained by the data controller; it can be obtained by one controller also on behalf of a joint controller (or another independent controller) when that is made clear to the subject and when that procedure has been specified in the contract between the controllers.

We reviewed informed consent forms from the five CIED manufacturers that were distributed by cardiologists and hospitals during

January and February 2019. Members of the Task Force provided the forms used in their own institutions and countries, and forms from other countries were obtained with the assistance of members of their national Cardiac Society. In total, 72 information sheets and consent forms used in 16 European countries were obtained and analysed systematically with respect to 20 criteria related to RM and storage of data, partnership, rights, data access, use of data for other purposes, anonymization, and legal responsibilities (Table 3). Consistency of approach between countries for each manufacturer was assessed by comparing their versions in different languages.

In most cases, the written information provided in consent forms was unclear with respect to how the data collected by RM are handled. One company did not define how many partners would have access to the data, while the other companies cited variable numbers. The party responsible for the data was not defined by one manufacturer and designated as both the physician and the hospital by the others. None defined clearly who should be considered the 'data controller'; specific responsibilities of each company regarding the data were not defined. Regarding storage of the data, no details were provided by two of the manufacturers. In four manufacturers' forms, the rights of the patient were not clearly explained; according to two manufacturers, the patients would not have access to their own data or be able to withdraw their consent.

In most cases, the duration of the contract was not defined; four manufacturers did not state for how long the patient's data would be

Table 3 Review of consent forms for remote monitoring of CIEDs

	Abbot	Biotronik	Boston Scientific	Medtronic	Microport
Clear definition of remote monitoring	A few aspects are not clear	Most aspects are clearly defined	Most aspects are clearly defined	Some aspects are not well defined	Many aspects are not defined
Clear explanation of how the data will be treated	No	No	Yes	No	No
Numbers of partners	Doctor, hospital, the company, and partners	Doctor, service partners	Doctor, hospital, the company, and partners	Patient, doctor, hospital, and third party	Not defined
Duration of the contract	Not defined	Not defined	6 years after the disconnection	Not defined	Not defined
Who is the responsible for the data?	Physician, hospital	Physician	The hospital/clinic	Not defined	Hospital
Who is responsible for the personal data?	Physician, hospital	Physician	The hospital/clinic	Medical centre	Hospital
Who will have access to the data?	The company, a third party, doctor, and hospital	Not defined	The company, subcontractors, doctor, or other physician who will grant access, your hospital, health authorities	The company, third party. The roles of the doctor and hospital are not defined	Doctor, hospital, the company, and the patient
Will the data be stored outside the hospital?	Yes, USA	Not defined	Yes	Yes	Not defined
Who will store the data?	The company	Not defined	The company and subcontractors	The company and a third party	Not defined
Are the rights of the patient clearly explained?	No	No	Yes	No	No
Does the patient have access to the data and/or to withdraw consent? Is that process well defined?	No. Even if patient withdraws consent, his/her data will be used for 10 years.	Yes, but the process is not defined	Yes	Yes, by writing a letter to the physician	Yes
Will data be used for statistics or research purposes?	Yes	Medical technical research	Yes previous anonymization	Yes	Not defined
Is the responsibility of each party established (manage the data, database, maintenance of the data obtained, software)?	No	No	No	No	No
Is there clear identification of data that will be obtained, from the clinic, device, personal contact of the patient?	No	No	Yes	Yes	No

Continued

Table 3 Continued

	Abbot	Biotronic	Boston Scientific	Medtronic	Microport
Data access is clearly defined and justified	The company, a third party, doctor, and hospital	Medical technical research	The company, subcontractors, doctor, or other physician that will grant access, your hospital, health authorities	Yes	No
How long will the company keep the data	Not defined	Not defined	At least 6 years or more after the end of the service	Not defined	Not defined
Where will the data be stored (EU)?	USA	Not defined	Ireland and USA	The local country, Netherlands, and USA	Not defined
The patient has the choice of different options regarding the informed consent	No	No	Yes, (i) the data of the patient, (ii) the medical data and (iii) statistical purposes and research	No	No
In case of research purposes, the data will be anonymized	Yes	Yes	Yes	Yes	Not defined
Right to withdraw informed consent	Yes	Not defined	Contact the company, email or postal letter to the company or your hospital	Yes	Only the data of identification, not defined the medical data
Definition of the time of analysis of data	No, only in case of withdrawal of the consent	Yes, during the working period of your doctor	No	No	Not defined
The utility is defined	Yes	Yes, only optimization of your treatment	Yes	Yes	Not clearly defined
Identification of the technical limitations of remote monitoring	No	Only those limitations linked to telephone networks	No	No	No
If more information is needed, is any web address or file offered?	No	No, contact the physician	No	No	No
Description of the limitations of the systems	No	Telecommunication systems of mobile phone	No	No	No
Are the informed consent forms consistent across countries?	No	No	No	No	No

Consent forms from five CIED manufacturers provided by cardiologists and manufacturers in January and February 2019 were reviewed. CIED, cardiac implantable electronic device.

retained. Four manufacturers stated that any data used for research would be anonymized. Only one form described any technical limitations of RM. No links to websites or sources of further information were provided. In all cases, the informed consent varied within each company between languages and countries, regarding structure, readability and content. For example, one company disclosed in the information provided in one country and language, where the patient's data would be stored, but it did not provide the same information in its forms used in other countries.

This analysis of documents from 16 countries may not reflect the situation throughout Europe. Until the GDPR was implemented, each country had to adopt its own methods to meet the requirements of the previous EU Directive. It is possible that some companies were still in the process of revising their consent forms and that some hospitals had not integrated the most recent versions in their daily practice. Some healthcare providers may be using informed consent forms created by themselves after discussion with each company. Some companies may have modified their consent forms since the review conducted by this Task Force was performed.

We have not determined how the readability of the consent forms relates to the average educational level and literacy of patients in each country, but most forms use some technical language without detailed definitions. None uses drawings or illustrations to explain the RM. Some forms include sections printed densely in very small fonts that are unlikely to be legible to many older patients who require CIEDs; we found lettering as small as five points (1 mm) in height, provided by one company but only in the versions of its form used in selected countries. If these issues are common and patients have a limited understanding of what they are asked to sign, then it could be argued that their consent is invalid.

In the construction of a generic information sheet and sample consent form for RM, this Task Force included advice from CIED-patients.

Cybersecurity and remote monitoring of cardiac implantable electronic devices

As implantable medical devices have evolved, manufacturers have reduced their size and weight, and now these devices rely critically on software to carry out their functions and they have become more interconnected. While cybersecurity is not the principal focus of this report, it is important for physicians to have some basic understanding of the main issues, especially because they have to discuss RM with their patients when they seek consent. Some basic terms relating to the cybersecurity of personal data are defined in [Supplementary material online, Appendix S3](#). A Medical Device Coordination Group Document from the European Commission provides comprehensive guidance for manufacturers so that they can meet stringent security requirements when designing implantable medical devices.²⁷

Current CIEDs contain a radio interface enabling wireless communication with external device programmers or base stations, thereby allowing the telemetry of data and the non-invasive reprogramming

of device settings. These provide many benefits for patients but the increased amount of software and interfaces on CIEDs significantly broaden their attack surface and expose them to new threats.²⁸ Recent studies by security researchers have demonstrated that it is possible to exploit both the wireless interface^{29–35} and the analogue interface³⁶ (the sensors and actuators inside the CIED) to execute attacks against implanted medical devices including CIEDs.^{29–31,36} To date, wireless attacks are more relevant since they are easier to launch, while analogue attacks can only be conducted successfully from a distance up to 5 cm in certain conditions that are difficult to be met in practice.³⁶

Regarding wireless attacks against CIEDs, there have been several reports of serious security weaknesses in the proprietary (non-standard) wireless protocols used by external devices to communicate with CIEDs.^{30–31} These studies include practical demonstrations of how to exploit these vulnerabilities through *in vitro* yet realistic laboratory experiments. While there have been no known *in vivo* attacks against patients so far, attackers could easily exploit the wireless nature of the communications between the patient's CIED and the external devices, not only to intercept the transmitted data but also to send maliciously crafted messages to the patient's CIED. The consequences of such attacks could be significant for patients, potentially compromising their privacy or modifying the functions of their device. As a consequence of these reports, a safety communication was issued by the Food and Drug Administration in the USA in March 2019, alerting users to cybersecurity vulnerabilities because a telemetry protocol did not use encryption, authentication, or authorization.³⁷

One important lesson to learn from the published studies is that CIED manufacturers typically rely on keeping the specifications of their wireless protocols secret, as their only means to provide 'security'.^{28,29} This (insecure) approach is known as 'security through obscurity' since it assumes that attackers who do not have access to a protocol's specifications will be unable to learning its inner workings. Several researchers, however, have shown that generally proprietary protocols can be broken without prior knowledge, thus rendering them fully insecure. The only solution to protect the data transmitted between the patient's CIED and the external device is using cryptography with other measures.³⁸ Cardiac implantable electronic device manufacturers can migrate from their weak, insecure proprietary protocols to strong security solutions that have been well scrutinized by security researchers, and then use these solutions according to standard security guidelines.

International comparisons

Remote monitoring has become standard of care in the USA for patients with CIEDs since the publication in 2015 of a consensus document by the HRS.¹² Between 2006 and 2010, approximately 50% of US patients with CIEDs capable of RM were actively monitored in this way³⁹ and that proportion is increasing. Lack of use of RM relates mainly to the local practice environment rather than to individual patient characteristics.

The timing of initiation of RM and education of the patient and caregivers varies between institutions. Patients typically receive the

remote transceiver at the time of hospital discharge following the implant surgery or at their first post-operative visit. Educational information is provided to the patient and caregivers to ensure that they understand the benefits and limitations of RM, how to set up the transceiver, that their physician or another healthcare professional will contact them if a significant abnormality is detected, and what the arrhythmia service expects of them to ensure that the collaboration is effective. While obtaining a signed informed consent form is not mandatory in the USA before starting RM, the HRS has created a patient information sheet that clinics may use to aid this effort.⁴⁰

Unless patients ask about the pathway for flow of their data, the companies or other entities involved in collecting, transmitting or storing their data will not typically be discussed. Healthcare providers and patients in the USA are focused on implementing RM effectively and to date, they have not demonstrated significant concern or apprehension regarding protection of the data generated by their CIED and then shared across the internet. There is official guidance⁴¹ but manufacturers often do not include details about cybersecurity in their product summaries.⁴²

Principles of informed consent

The primacy of the ethical principle of respecting each patient's autonomy was enshrined by the most recent revision of the Declaration of Geneva by the World Medical Association.⁴³ Patients must be given as much information as they wish or need to have in order to make informed decisions.⁴⁴ The European Data Protection Supervisor has stated recently that consent as the legal basis for processing data according to the GDPR 'must be freely given, specific, informed, and unambiguous'.⁴⁵ For consent to be valid, information should be given in language that is readily interpretable by patients who have no special medical or technical knowledge, and in a format that is easily legible. Evidence from a cardiology study suggested that often this is not the case,⁴⁶ and our review has revealed similar divergences from optimal practice.

Insights from behavioural science can guide us.⁴⁷ To achieve effective and good-quality decision-making by the patient, the doctor or other healthcare professional must be involved in the discussion.^{48,49} In general, engaging the patient in making decisions leads to better clinical outcomes.⁵⁰ Anxiety can be reduced and the recall of information increased if patient decision aids are used;⁵¹ for example patients who underwent cardiac catheterization were less anxious and better informed if they were randomized to receive information in a pictorial format.⁵²

In the specific context of CIEDs, further research would be valuable to explore how well patients understand how their devices are monitored and how their data are transmitted, processed and shared. A recent study showed that patients received less knowledge than they expected and wanted.⁴⁹ One model that suggests how the process could be improved is that of dynamic consent, meaning that the patient can give consent for different components of their care in separate stages and at different times, under their own control and with access to additional information if and when they wish it; the model is described as seeing patients as 'partners' rather than as 'subjects'.⁵³ Finland is one interesting example, where patients have

secure access via the internet to all their healthcare records in the Patient Data Repository, and each citizen has to consent how their data can be shared between various healthcare units.⁵⁴ The ethical principle should be that the patient controls their own data, and gives access implicitly when consulting a physician or other healthcare professional but explicitly for any other purpose.

Recommendations

A thorough understanding, not only of their technical functions but also of the regulatory framework applicable to medical devices is essential for the delivery of state-of-the-art care and for compliance with the current GDPR. Physicians and healthcare providers should also be aware of vulnerabilities and of general strategies for enhancing cybersecurity.⁵⁵

Manufacturers of CIEDs may not need, and may not want to obtain, personalized data but they must collect device performance data. It is therefore recommended that manufacturers should always collect and process the minimum amount of identifiable data necessary, and wherever feasible have access to pseudonymized data only, traceable when required to a linked unique device identification (UDI). For certain technical analyses, fully anonymized data will be sufficient.

In the view of this Task Force, consensus recommendations need to be developed concerning which data are collected and exchanged. European Heart Rhythm Association is collaborating with the Heart Rhythm Society and manufacturers to develop compatible protocols.⁵⁶ The following recommendations relate specifically to the requirements of the EU GDPR, the cybersecurity of CIEDs, and the implications for obtaining informed consent:

Interpretation and implementation of the General Data Protection Regulation

- (1) Manufacturers are data controllers if they establish the objectives ('purposes') for RM of their devices, if they determine which data should be collected, and if they develop the methods ('means') for obtaining those data. They may also act as data processors when analysing and storing the data collected, but they are not only processors on behalf of hospitals because of their roles in determining the objectives and methods of RM.
- (2) Hospitals are also data controllers since they determine the clinical indications for collecting data remotely from CIEDs, the details of the procedure, and which data are collected and analysed from individual patients.
- (3) The Task Force recommends that only hospitals should be capable to convert pseudonymized device data into patient-specific information. Physicians and other healthcare professionals employed by the hospital review the data provided by the manufacturer or third-party provider; they may then implement any indicated clinical decisions, they may store the data, and they can initiate and conduct secondary analyses of the data.
- (4) The most appropriate model is that of two joint controllers. This requires a legal contract between the joint controllers that specifies their respective responsibilities and liabilities. A model framework for a contract is available as [Supplementary material online, Appendix S4](#).

- (5) Independent cardiologists who are self-employed need to be considered as data controllers if they work in private practice or as private/independent practitioners in a hospital.
- (6) Third-party providers are data processors if they function under delegated authority from a data controller to collect, analyse, and transmit data acquired from RM of CIEDs. An agreement between the controller and the processor must be drafted; topics to be mentioned in the agreement are given in [Supplementary material online, Appendix S5](#).
- (7) Specific guidance is needed from the European Data Protection Board concerning the balance between the requirements of the EU Data Protection Regulation (allowing patients individual control of their own data) and the requirements of the EU Medical Device Regulation (requiring manufacturers to undertake surveillance of their high-risk medical devices). Legal guidance from the European Commission could clarify issues relating to the use of personal data from medical registries and clinical databases, for secondary research. A preliminary opinion from the European Data Protection Supervisor on data protection and scientific research, published in January 2020, states that further work to develop codes of conduct is required.⁴⁵

Cybersecurity

- (1) Manufacturers should implement secure encrypted communication protocols between an implanted CIED and its local transceiver. Manufacturers should disclose in general terms what security measures they take.
- (2) All data transferred via the internet or cloud to manufacturers, third-party providers, and hospitals, should also be encrypted or secured by any other means.
- (3) The European Commission should establish and support an Expert Laboratory to conduct vulnerability testing of internet-enabled medical devices, according to the provisions of the EU Regulation on Medical Devices.

Informed consent

- (1) The Task Force recommends that obtaining consent both for the implantation of a CIED and for its RM should be initiated as a single procedure, and optimally *before* the device is implanted. This should be the responsibility of the hospital, which should retain a copy of the consent form.
- (2) Information for patients must be provided in non-technical terms in their native language. The description of the implant and its monitoring must be readily interpretable by people with average literacy. Infographics are better understood than large bodies of text. Small font sizes must not be used.⁵⁷
- (3) Information provided to patients should include how their data are transmitted, how safety of the process is ensured, and with whom and for what purposes the data are shared. The information prepared by manufacturers for patients in the Summary of Safety and Clinical Performance⁵⁸ that will now be available for every high-risk implantable medical device including CIEDs should include details of remote monitoring.
- (4) A generic information sheet and sample consent form is available as [Supplementary material online, Appendix S6](#). This can be customized for specific local requirements or for particular devices and new technology, but it will always be important to explain RM in simple non-legal language and to provide answers to all frequently asked questions.

- (5) Patients should be allowed to access their own data collected by RM. Manufacturers should investigate with hospitals how this could be provided, perhaps using a common portal that could also be used for dynamic consent.⁵⁹ The draft European Strategy for Data states that there is a lack of tools for empowering individuals in enforcing their rights under the GDPR, such as 'web-based interfaces for requesting access to personal data'.⁶⁰

Supplementary material

Supplementary material is available at *Europace* online.

Acknowledgements

We thank Ilaria Leggeri for her expert and efficient support for this Task Force; Enrico Caiani and Deborah Mascalzoni for reviewing the manuscript; and Savontaus Mikko (Finland), Daniele Muser (Italy), Dominic A.M.J. Theuns (Netherlands), Ricardo Fontes Carvalho (Portugal), Gonzalo Rodrigo Trallero (Spain), Rafael Vidal Pérez (Spain), Michael Doering (Germany), and Juhlin Tord (Sweden) for providing informed consent forms from their respective countries. We thank Andrew Locker (UK) and Axel Verstrael (Germany) for their helpful contributions from the perspective of patients.

Conflict of interest: J.C.N. is supported by grants from the Novo Nordisk Foundation (NNF16OC0018658 and NNF17OC0029148). J.K. has received speaker's honoraria from Boehringer Ingelheim, Biosense Webster, Biotronik, Boston Scientific, Daiichi Sankyo, Medtronic, Merck Sharp & Dohme, Pfizer, and Abbott—St. Jude Medical; and has served as a consultant for Bayer, Boehringer Ingelheim, Biosense Webster, Boston Scientific, Daiichi Sankyo, Medtronic, Merit, MicroPort, and Abbott—St. Jude Medical. R.C.A. has received speaker's honoraria from Boston Scientific and Bayer. H.B. has received institutional fellowship and research grant support from Abbott, Biotronik, Boston Scientific, Medtronic, and Microport, and speaker fees from Biotronik and Medtronic. M.R.C. has received research funding and personal fees from Abbott, Medtronic and Boston Scientific. ID is an employee of the European Society of Cardiology. V.K. has received research grants from Boston Scientific, Biotronik, ZOLL Inc., and Spire Inc., and honoraria from ZOLL Inc. and Biotronik. A.K. is an employee of Biotronik and K.S. is an employee of Boston Scientific. H.H. has received no personal funding, and discloses institutional support as unconditional research grants from Medtronic, Daiichi Sankyo, Boehringer-Ingelheim, Bayer, Pfizer-BMS, Biotronik, Abbott, and Bracco Imaging. All other authors declared no conflicts of interest.

References

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L 119, 4 May 2016. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN> (26 June 2020, date last accessed).
2. Burri B, Senouf D. Remote monitoring and follow-up of pacemakers and implantable cardioverter defibrillators. *Europace* 2009;**11**:701–9.
3. Dubner S, Auricchio A, Steinberg JS, Vardas P, Stone P, Brugada J et al. ISHNE/EHRA expert consensus on remote monitoring of cardiovascular implantable electronic devices (CIEDs). *Europace* 2012;**14**:278–93.

4. Cheng A, Landman SR, Stadler RW. Reasons for loss of cardiac resynchronization therapy pacing: insights from 32844 patients. *Circ Arrhythm Electrophysiol* 2012;**5**:884–8.
5. Varma N, Jones P, Wold N, Cronin E, Stein K. How well do results from randomized clinical trials and/or recommendations for implantable cardioverter-defibrillator programming diffuse into clinical practice? Translation assessed in a national cohort of patients with implantable cardioverter-defibrillators (ALITUDE). *J Am Heart Assoc* 2019;**8**:e007392.
6. Shakibfar S, Krause O, Lund-Andersen C, Aranda A, Moll J, Andersen TO *et al*. Predicting electrical storms by remote monitoring of implantable cardioverter-defibrillator patients using machine learning. *Europace* 2019;**21**:268–74.
7. Boersma L, Barr C, Knops R, Theuns D, Eckardt L, Neuzil P *et al*; EFFORTLESS Investigator Group. Implant and midterm outcomes of the subcutaneous implantable cardioverter-defibrillator registry: the EFFORTLESS Study. *J Am Coll Cardiol* 2017;**70**:830–41.
8. Parthiban N, Esterman A, Mahajan R, Twomey DJ, Pathak RK, Lau DH *et al*. Remote monitoring of implantable cardioverter-defibrillators: a systematic review and meta-analysis of clinical outcomes. *J Am Coll Cardiol* 2015;**65**:2591–600.
9. Ontario HQ. Remote monitoring of implantable cardioverter-defibrillators, cardiac resynchronization therapy and permanent pacemakers: a health technology assessment. *Ont Health Technol Assess Ser* 2018;**18**:1–199.
10. Hindricks G, Varma N, Kacet S, Lewalter T, Søgaard P, Guédon-Moreau L *et al*. Daily remote monitoring of implantable cardioverter-defibrillators: insights from the pooled patient-level data from three randomized controlled trials (IN-TIME, ECOST, TRUST). *Eur Heart J* 2017;**38**:1749–55.
11. Brignole M, Auricchio A, Baron-Esquivias G, Bordachar P, Boriani G, Breithardt OA *et al*. 2013 ESC guidelines on cardiac pacing and cardiac resynchronization therapy: the task force on cardiac pacing and resynchronization therapy of the European Society of Cardiology (ESC). Developed in collaboration with the European Heart Rhythm Association (EHRA). *Europace* 2013;**15**:1070–118.
12. Slotwiner D, Varma N, Akar JG, Annas G, Beardsall M, Fogel RI *et al*. HRS Expert Consensus Statement on remote interrogation and monitoring for cardiovascular implantable electronic devices. *Heart Rhythm* 2015;**12**:e69–100.
13. Varma N, Epstein AE, Irimpen A, Schweikert R, Love C; for the TRUST Investigators. Efficacy and safety of automatic remote monitoring for implantable cardioverter-defibrillator follow-up. *Circulation* 2010;**122**:325–32.
14. Mairesse GH, Braunschweig F, Klersy K, Cowie MR, Leyva F. Implementation and reimbursement of remote monitoring for cardiac implantable electronic devices in Europe: a survey from the health economics committee of the European Heart Rhythm Association. *Europace* 2015;**17**:814–8.
15. Vinck I, De Laet C, Stroobandt S, Van Brabant H. Legal and organizational aspects of remote cardiac monitoring: the example of implantable cardioverter defibrillators. *Europace* 2012;**14**:1230–5.
16. Article 29 Data Protection Working Party. Opinion 1/2010 on the concepts of “controller” and “processor”. 00264/10/EN, WP 169. European Commission, Directorate General Justice, Freedom and Security, adopted on 16 February 2010. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf (18 August 2019, date last accessed).
17. Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC. Recital 67. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2014_158_R_0001 (10 January 2018, date last accessed).
18. Leonard T, Guerguinov O. *Surveillance à distance des dispositifs cardiaques implantés et protection des données*. Brussels: Ulys; 2019.
19. See articles 44–50 GDPR (reference 1).
20. European Union. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2017.117.01.0001.01.ENG&toc=OJ:L:2017:117:TOC (29 October 2019, date last accessed).
21. Harmon SH, Haddow G, Gilman L. New risks inadequately managed: the case of smart implants and medical device regulation. *Law Innov Technol* 2015;**7**:231–52.
22. Petersen HH, Larsen MC, Nielsen OW, Kensing F, Svendsen JH. Patient satisfaction and suggestions for improvement of remote ICD monitoring. *J Interv Card Electrophysiol* 2012;**34**:317–24.
23. Timmermans I, Meine M, Szendey I, Aring J, Romero Roldán J, van Erven L *et al*. Remote monitoring of implantable cardioverter defibrillators: patient experiences and preferences for follow-up. *Pacing Clin Electrophysiol* 2018;**42**:120–9.
24. European Commission, Digital Single Market. mHealth in Europe: Preparing the ground—consultation results published. 2015. <https://ec.europa.eu/digital-single-market/en/news/mhealth-europe-preparing-ground-consultation-results-published> (1 November 2019, date last accessed).
25. European Commission. Results of the public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy. 2016. <https://ec.europa.eu/digital-single-market/en/news/results-public-consultation-regulatory-environment-platforms-online-intermediaries-data-and> (17 July 2019, date last accessed).
26. Hernandez-Madrid A, Lewalter T, Proclemer A, Pison L, Lip GYH, Blomstrom-Lundqvist C; Scientific Initiatives Committee, European Heart Rhythm Association. Remote monitoring of cardiac implantable electronic devices in Europe: results of the European Heart Rhythm Association survey. *Europace* 2014;**16**:129–32.
27. European Commission. Guidance on cybersecurity for medical devices. MDCC 2019-16, 2019. <https://ec.europa.eu/docsroom/documents/38941/attachments/1/translations/en/renditions/native> (10 April 2020, date last accessed).
28. Marin E. Security and privacy of implantable medical devices. PhD thesis. University of Leuven, 2018. <https://www.esat.kuleuven.be/cosic/publications/the-sis-302.pdf> (1 November 2019, date last accessed).
29. Marin E, Singelée D, Garcia FD, Chothia T, Willems R, Preneel B. On the (in)security of the latest generation implantable cardiac defibrillators and how to secure them. Proceedings of the 32nd Annual Conference on Computer Security Applications. 2016:226–36. http://delivery.acm.org/10.1145/3000000/2991094/p226-marin.pdf?ip=131.251.254.138&id=2991094&acc=ACTIVE%20SERVICE&key=BF07A2EE685417C5%2E8AEC776A404BE5B3%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&__acm__=1572607669_88075a53fb85388e44b696d0d4a53109 (1 November 2019, date last accessed).
30. Halperin D, Heydt-Benjamin TS, Ransford B, Clark SS, Defend B, Morgan W *et al*. Pacemakers and implantable cardiac defibrillators: software radio attacks and zero-power defenses. Proceedings of the 29th IEEE Symposium on Security and Privacy 2008:129–42.
31. Rios B, Butts J. Security evaluation of the implantable cardiac device ecosystem architecture and implementation interdependencies. WhiteScope; 2017. <https://www.ledecodur.ch/wp-content/uploads/2017/05/Pacemaker-Ecosystem-Evaluation.pdf> (1 November 2019, date last accessed).
32. Marin E, Singelée D, Yang B, Verbauwhe I, Preneel B. On the feasibility of cryptography for a wireless insulin pump system. Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy 2016:113–20. doi:10.1145/2857705.2857746. http://delivery.acm.org/10.1145/2860000/2857746/p113-marin.pdf?ip=131.251.254.138&id=2857746&acc=ACTIVE%20SERVICE&key=BF07A2EE685417C5%2E8AEC776A404BE5B3%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&__acm__=1572610253_f6e03b615f02fce94b4e1e8704b717c5 (1 November 2019, date last accessed).
33. Marin E, Singelée D, Yang B, Volskiy V, Vandenbosch G, Nuttin B *et al*. Securing wireless neurostimulators. Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy 2018:287–98. doi:10.1145/3176258.3176310. http://delivery.acm.org/10.1145/3180000/3176310/p287-marin.pdf?ip=131.251.254.138&id=3176310&acc=ACTIVE%20SERVICE&key=BF07A2EE685417C5%2E8AEC776A404BE5B3%2E4D4702B0C3E38B35&__acm__=1572610760_6ebd527ded5025db645e15a401fc0fee (1 November 2019, date last accessed).
34. Li C, Raghunathan A, Jha NK. Hijacking an insulin pump: security attacks and defenses for a diabetes therapy system. Proceedings of the 13th International Conference on e-Health Networking Applications and Services 2011:150–6. doi:10.1109/HEALTH.2011.6026732. <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6026732> (1 November 2019, date last accessed).
35. Reverberi L, Oswald D. Breaking (and fixing) a widely used continuous glucose monitoring system. Proceedings of the 11th USENIX Conference on Offensive Technologies (WOOT), 2017. <https://www.usenix.org/system/files/conference/woot17/woot17-paper-reverberi.pdf?CFID=81922470&CFTOKEN=96209d45978a25c6-84C33B63-E723-A52F-71E18D610C9F52D6> (1 November 2019, date last accessed).
36. Kune DF, Backes JD, Clark SS, Kramer DB, Reynolds MR, Fu K *et al*. Ghost Talk: Mitigating EMI signal injection attacks against analog sensors. Proceedings of the IEEE Symposium on Security and Privacy 2013:145–59. doi:10.1109/SP.2013.2. <https://ieeexplore.ieee.org/document/6547107/authors#authors> (1 November, date last accessed).
37. US Food and Drug Administration. Cybersecurity vulnerabilities affecting Medtronic implantable cardiac devices, programmers, and home monitors: FDA safety communication. 2019. <https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm633960.htm> (March 2019, date last accessed).
38. Pycroft L, Aziz TZ. Security of implantable medical devices with wireless connections: the dangers of cyber-attacks. *Exp Rev Med Dev* 2018;**15**:403–6.
39. Akar JG, Bao H, Jones P, Wang Y, Chaudhry SI, Varosy P *et al*. Use of remote monitoring of newly implanted cardioverter-defibrillators: insights from the patient related determinants of ICD remote monitoring (PREDICT RM) study. *Circulation* 2013;**128**:2372–83.
40. Heart Rhythm Society. <https://www.hrsonline.org/Patient-Resources/Patient-Information-Sheets> (24 April 2019, date last accessed).

41. US Food and Drug Administration. Postmarket management of cybersecurity in medical devices. Guidance for industry and Food and Drug Administration staff. 2016. <https://www.fda.gov/media/95862/download> (6 April 2020, date last accessed).
42. Stern AD, Gordon WJ, Landman AB, Kramer DB. Cybersecurity features of digital medical devices: an analysis of FDA product summaries. *BMJ Open* 2019;**9**:e025374.
43. Parsa-Parsi RW. The revised declaration of Geneva: a modern-day physician's pledge. *JAMA* 2017;**318**:1971–2.
44. Fraser AG, Butchart EG, Szymański P, Caiani EG, Crosby S, Kearney P et al. The need for transparency of clinical evidence for medical devices in Europe. *Lancet* 2018;**392**:521–30.
45. European Data Protection Supervisor. A preliminary opinion on data protection and scientific research. 2020. https://edps.europa.eu/data-protection/our-work/publications/opinions/preliminary-opinion-data-protection-and-scientific_en (8 April 2020, date last accessed).
46. Terranova G, Ferro M, Carpeggiani C, Recchia V, Braga L, Semelka RC et al. Low quality and lack of clarity of current informed consent forms in cardiology: how to improve them. *JACC Cardiovasc Imaging* 2012;**5**:649–55.
47. Vos IML, Schermer MHN, Bolt I. Recent insights into decision-making and their implications for informed consent. *J Med Ethics* 2018;**44**:734–8.
48. Stiggelbout AM, Pieterse AH, De Haes JCJM. Shared decision making: concepts, evidence, and practice. *Patient Educ Couns* 2015;**98**:1172–9.
49. Ingadottir B, Thylen I, Ulin K, Jaarsma T. Patients are expecting to learn more: a longitudinal study of patients with heart failure undergoing device implantation. *Patient Educ Couns* 2020;doi:10.1016/j.pec.2020.02.023.
50. Hughes TM, Merath K, Chen Q, Sun S, Palmer E, Idrees JJ et al. Association of shared decision-making on patient-reported health outcomes and healthcare utilization. *Am J Surg* 2018;**216**:7–12.
51. Scalia P, Durand MA, Berkowitz JL, Ramesh NP, Faber MJ, Kremer JAM et al. The impact and utility of encounter patient decision aids: systematic review, meta-analysis and narrative synthesis. *Patient Educ Couns* 2019;**102**:817–41.
52. Brand A, Gao L, Hamann A, Crayen C, Brand H, Squier SM et al. Medical graphic narratives to improve patient comprehension and periprocedural anxiety before coronary angiography and percutaneous coronary intervention: a randomized trial. *Ann Intern Med* 2019;**170**:579–81.
53. Budin-Ljøsne I, Teare HJ, Kaye J, Beck S, Bentzen HB, Caenazzo L et al. Dynamic consent: a potential solution to some of the challenges of modern biomedical research. *BMC Med Ethics* 2017;**18**:4.
54. Kanta. Medical records. <https://www.kanta.fi/en/medical-records> (27 July 2019, date last accessed).
55. Baranchuk A, Refaat MM, Patton KK, Chung MK, Krishnan K, Kutiyifa V et al. American College of Cardiology's Electrophysiology Section Leadership. Cybersecurity for cardiac implantable electronic devices: what should you know? *J Am Coll Cardiol* 2018;**71**:1284–8.
56. Slotwiner DJ, Abraham RL, Al-Khatib SM, Anderson HV, Bunch TJ, Ferrara MG et al. HRS White Paper on interoperability of data from cardiac implantable electronic devices (CIEDs). *Heart Rhythm* 2019;**16**:e107–27.
57. Paasche-Orlow MK, Taylor HA, Brancati FL. Readability standards for informed-consent forms as compared with actual readability. *N Engl J Med* 2003;**348**:721–6.
58. European Commission, Medical Device Coordination Group Document MDCG 2019–9. Summary of safety and clinical performance. A guide for manufacturers and notified bodies. August 2019. <https://ec.europa.eu/docsroom/documents/37323?locale=en> (29 October 2019, date last accessed).
59. Kaye J, Whitley EA, Lund D, Morrison M, Teare H, Melham K. Dynamic consent: a patient interface for twenty-first century research networks. *Eur J Hum Genet* 2015;**23**:141–6.
60. European Commission. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European Strategy for Data (draft). https://www.politico.eu/wp-content/uploads/2020/01/POLITICO_Data-strategy.pdf (10 April 2020, date last accessed).