Dálková monitorace implantovaných elektronických přístrojů v kardiologii. Zákonné požadavky a etické principy – společné stanovisko Pracovní skupiny Výboru pro regulační záležitosti Evropské kardiologické společnosti a Evropské asociace srdečního rytmu.

Překlad dokumentu připravený Českou kardiologickou společností

(Remote monitoring of cardiac implanted electronic devices: legal requirements and ethical principles – ESC Regulatory Affairs Committee/EHRA joint task force report. Translation of the document prepared by the Czech Society of Cardiology)

Miloš Táborský[a], Josef Kautzner[b], Hanka Wünschová[b], Lucie Nečasová[b], Marián Fedorco[a], Pavel Bradáč[a], Antonín Hlavinka[a], Petr Šustek[c]

[a] *Národní telemedicínské centrum, Fakultní nemocnice Olomouc, Olomouc*
[b] *Klinika kardiologie, Institut klinické a experimentální medicíny, Praha*
[c] *Katedra medicínského práva, Právnická fakulta Univerzity Karlovy, Praha*

Autoři originálního textu Pracovní skupiny Výboru pro regulační záležitosti Evropské kardiologické společnosti a Evropské asociace srdečního rytmu:[1] Jens Cosedis Nielsen, Josef Kautzner, Ruben Casado-Arroyo.

Tento přeložený reprint je publikován Českou kardiologickou společností a tvořen textem vybraným a přeloženým Českou kardiologickou společností z textu původně publikovaného v angličtině v „EP Europace 2020;22(11):1742–1758, doi:10.1093/europace/euaa168“ („časopise“) vydavatelstvím Oxford University Press v zastoupení Evropské kardiologické společnosti (European Society of Cardiology, ESC).

Adresa pro korespondenci: Prof. MUDr. Miloš Táborský, CSc., FESC, FACC, MBA, Národní telemedicínské centrum, Fakultní nemocnice Olomouc, I. P. Pavlova 6, 779 00 Olomouc, e-mail: milos.taborsky@fnol.cz
DOI: 10.33678/cor.2021.019

Tento článek prosím citujte takto: Táborský M, Kautzner J, Wünschová H, et al. Dálková monitorace implantovaných elektronických přístrojů v kardiologii. Zákonné požadavky a etické principy – společné stanovisko Pracovní skupiny Výboru pro regulační záležitosti Evropské kardiologické společnosti a Evropské asociace srdečního rytmu. Překlad dokumentu připravený Českou kardiologickou společností. Cor Vasa 2021;63:95–110.

INFORMACE O ČLÁNKU

Historie článku:
Vložen do systému: 24. 1. 2021
Přijat: 31. 1. 2021
Dostupný online: 1. 2. 2021

Klíčová slova:
Dálková monitorace
EHRA (Evropská asociace srdečního rytmu)
Formulář informovaného souhlasu
Implantabilní elektronický přístroj v kardiologii
Informovaný souhlas
Kybernetická bezpečnost
Obecné nařízení o ochraně soukromých údajů
Společný správce údajů
Správce údajů
Výbor ESC pro regulační záležitosti
Zpracovatel údajů

SOUHRN

Obecné nařízení o ochraně soukromých údajů (General Data Protection Regulation, GDPR) Evropské unie (EU) stanovuje právní odpovědnost při shromažďování a zpracování osobních informací o osobách žijících v EU. Tento dokument má zvláštní důsledky pro dálkové monitorování implantovaných elektronických přístrojů v kardiologii (cardiac implantable electronic device, CIED). Tato zpráva společné pracovní skupiny Evropské asociace pro srdeční rytmus (European Heart Rhythm Association) a Výboru pro regulační záležitosti Evropské kardiologické společnosti (European Society of Cardiology, ESC) doporučuje jednotný právní výklad GDPR. Výrobce i nemocnice je nutno považovat za společné správce údajů shromážděných dálkovým monitorováním (v závislosti na architektuře systému) a musejí mít uzavřenu vzájemnou smlouvu definující jejich příslušné úlohy; byla vypracována obecná předloha této smlouvy. Alternativou k tomuto uspořádání jsou dva nezávislí správci. Správci údajů jsou i kardiologové v soukromé praxi. Poskytovatelé monitorovacích platforem jako třetí strana mohou působit jako zpracovatelé údajů. Výrobci musejí vždy shromažďovat a zpracovávat minimální objem nezbytných identifikovatelných údajů, a kdykoli je to možné, mít přístup pouze k pseudonymizovaným údajům. Byla popsána zranitelná místa v oblasti kybernetické bezpečnosti při přenosu údajů mezi implantovaným přístrojem u pacienta a vysílačem/přijímačem; výrobci proto musejí používat bezpečné komunikační protokoly. Pacienty je třeba informovat o nakládání s jejich dálkově monitorovanými údaji a jejich použití, a ještě před implantací přístroje je nutno získat jejich informovaný souhlas. Rozbor v současnosti používaných formulářů souhlasu odhalilo velké rozdíly v jejich délce a obsahu a někdy i používání velmi odborných výrazů; proto byl navržen standardní informační list a obecný formulář souhlasu. Kardiologové pečující o pacienty s dálkově monitorovanými CIED by měli mít o těchto otázkách povědomí.

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

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.

Překlad je oficiálním dokumentem platformy e-Health České asociace preventivní kardiologie České kardiologické společnosti.

Úvod

Obecné nařízení o ochraně osobních údajů (General Data Protection Regulation, GDPR), které vstoupilo v platnost v Evropské unii (EU) v roce 2018, představuje společný právní rámec ve všech členských zemích. Toto nařízení reguluje, jak lze osobní informace shromažďovat a jak se s nimi musí nakládat. Poskytuje také jednoznačnou strukturu odpovědnosti v případě ohrožení bezpečnosti údajů nebo pokud má nějaká osoba dotazy či obavy v tomto ohledu, případně se rozhodne své osobní údaje již dále nesdílet.

Technologický pokrok dovoluje, aby stále větší počet pacientů využíval přínos dálkové monitorace (remote monitoring, RM) jejich zdravotnických prostředků (přístrojů). Výsledkem je obrovský objem osobních zdravotních údajů cirkulujících ve vzájemně propojených systémech. To platí zvláště pro implantabilní elektronické přístroje v kardiologii (cardiac implantable electronic device, CIED), jako jsou implantabilní kardiovertery-defibrilátory (ICD), kardiostimulátory (KS), přístroje pro srdeční resynchronizační léčbu (SRL) a smyčkové záznamníky, u nichž je RM již běžnou praxí. Jedinci mají právo kontrolovat, kdo má přístup k jejich osobním údajům a jak se používají. Pacienti jsou proto žádáni o podpis formulářů souhlasu, které umožňují výrobcům mít na dálku přístup k pacientovým údajům z výše uvedených přístrojů a v některých případech i sdílet tyto údaje se třetími stranami.

V roce 2018 vytvořily Výbor pro regulační záležitosti (Regulatory Affairs Committee) Evropské kardiologické společnosti (European Society of Cardiology, ESC) a Evropská asociace srdečního rytmu (European Heart Rhythm Association, EHRA) pracovní skupinu zaměřenou na otázky dálkového monitorování CIED. Členy této pracovní skupiny byli i představitelé výrobců a Heart Rhythm Socie-

ty (HRS). Jak se údaje kódují a jak se přenášejí, kam putují identifikovatelné informace, kdo s nimi pracuje a s kým jsou sdíleny? Kdo je odpovědný za samotné údaje a jejich zpracování a jak by se měl získávat informovaný souhlas? Platí pro lékaře v klinické praxi nějaká zvláštní právní odpovědnost? Jsou standardy uplatňovány poskytovateli zdravotní péče a výrobci systematicky? Tento dokument se zabývá uvedenými otázkami a doporučuje standardní postupy, které mohou nemocnice i jednotliví lékaři přijmout s cílem plnit své povinnosti podle GDPR.

Dálkové načtení dat a monitorování implantabilních elektronických přístrojů v kardiologii

Průkopníkem v oblasti dálkové správy CIED je společnost Biotronik (Berlín, Německo), která zavedla svůj systém nazvaný Home Monitoring® v roce 2001. V současné době nabízejí dálkovou správu přístrojů všichni výrobci, což zahrnuje hladký přenos údajů sítí z místa pobytu pacienta přes centrální databázi do nemocnice nebo ordinace lékaře. Alternativně mohou zpracovávat údaje pro třídění varovných upozornění nebo centralizaci přenášených souborů od různých výrobců na společné platformě poskytovatelé z třetí strany. Tyto údaje zahrnují funkční stav přístroje i údaje monitorované přístrojem od pacienta.

Sledování pacienta na dálku, které nahrazuje plánované návštěvy lékaře v ordinaci, je třeba odlišit od RM s automatickým neplánovaným přenosem varovných upozornění na předem specifikované nežádoucí příhody, jako jsou arytmie nebo abnormální impedance elektrod. Liší se i od pacientem spuštěného přenosu údajů či neplánovaných kontrol spuštěných manuálně samotným pacientem kvůli skutečné nebo domnělé klinické příhodě. Prvořadým cílem je zlepšit prognózu pacientů díky časné detekci příhod a aktivnímu řešení situace.

Přehled mezinárodních standardů týkajících se RM lze nalézt v doplňkovém materiálu online (příloha S1). Dálkové monitorování nabízí platformu pro uchovávání a analýzu údajů s obrovským množstvím informací, jichž lze využít jak pro péči v klinické praxi, výzkum, tak pro kontrolu technických parametrů CIED. Výrobci používají údaje získané z RM jako inspiraci pro neustálé zdokonalování přístrojů i ke zvýšení účinnosti a snížení nákladů na klinické vyšetření. Například údaje získané z RM subkutánních ICD umožnily vývoj nového algoritmu snižujícího nesprávně indikované výboje o 70 %. Dálkové monitorování rovněž poskytuje údaje, které musejí výrobci shromažďovat pro zajištění dlouhodobé bezpečnosti a spolehlivého fungování jejich přístrojů.

Klinický přínos RM byl předmětem řady publikovaných prací. Podle doporučených postupů EHRA/ESC z roku 2013 je RM doporučením třídy IIa (úroveň důkazů A), které zajišťuje časnější detekci klinických i technických problémů. V pozdějším konsenzuálním dokumentu expertů HRS se konstatuje, že RM by měla být nabídnuta všem pacientům s CIED jako součást standardního sledování (třída doporučení I, úroveň důkazů A). Dokument hodnotící zdravotnické technologie dospěl k závěru, že RM CIED pro sledování aktuálního zdravotního stavu pacienta a monitoraci přístroje je výhodná z hlediska vynaložených nákladů. Studie TRUST prokázala, že RM je sice bezpečnou metodou, protože není spojena se zvýšenou morbiditou, ale je potřeba dále studovat dopad RM na klinické výsledky a prognózu pacientů. Navzdory těmto doporučením se zatím dálková správa v Evropě používá pouze u menšiny pacientů s CIED, zejména z důvodu chybějící úhrady. Z toho vyplývá, že RM by měly být financovány jako nedílná součást nepřetržité péče o pacienta. O nutnosti vypracování jistých pravidel k právním aspektům RM se ví již několik let.

Evropská nařízení pro dálkové monitorování implantabilních elektronických přístrojů v kardiologii

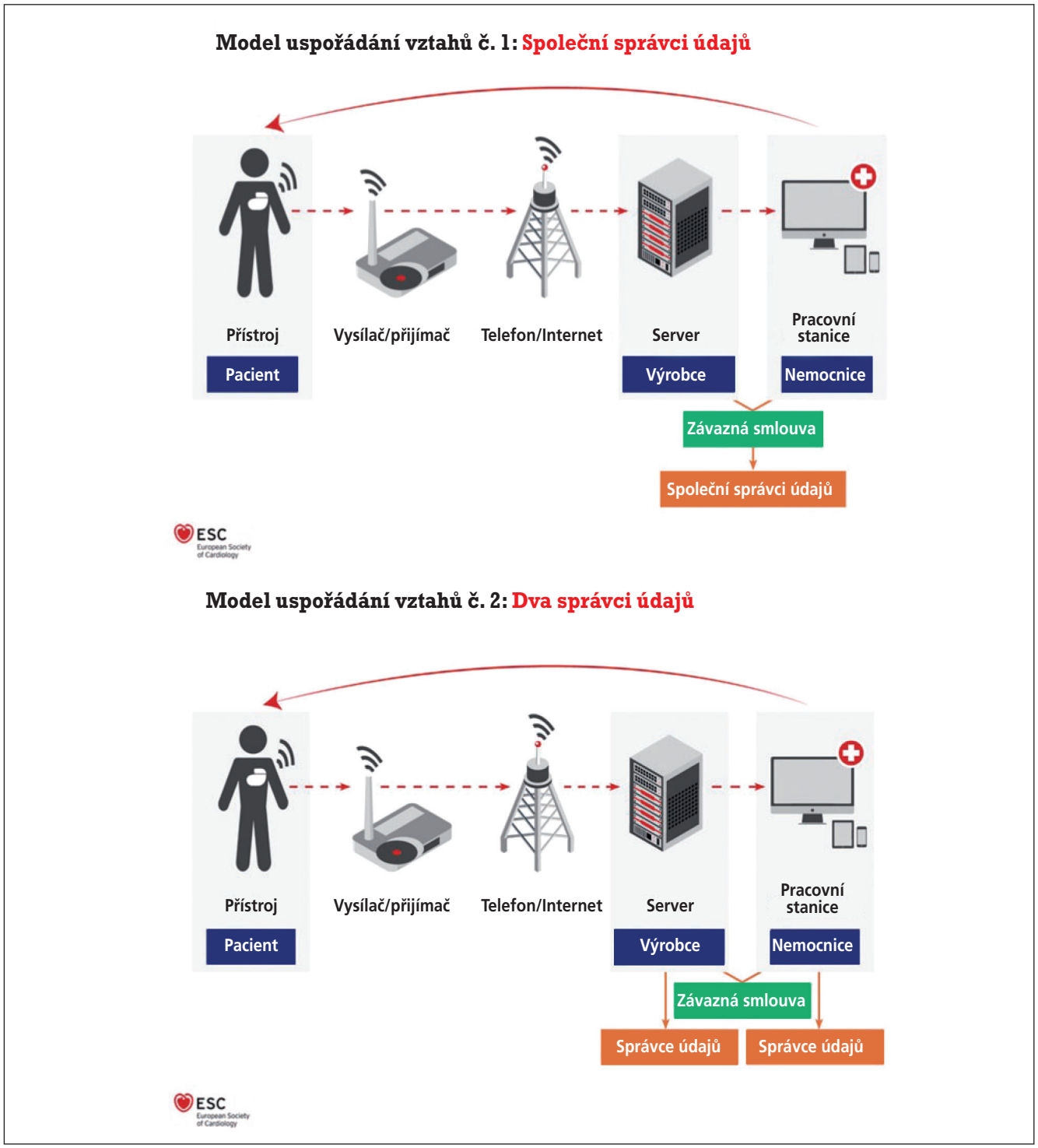
Nařízení Evropské unie o ochraně osobních údajů

Obecné nařízení o ochraně osobních údajů (GDPR) schválily Evropský parlament a Rada Evropské unie v roce 2016 a po přechodném období vstoupilo v platnost k 25. květnu 2018. Tato právní úprava nahradila směrnici o ochraně osobních údajů EU (Data Protection Directive) z roku 1995, u níž se dospělo k názoru, že již není v důsledku technologického pokroku aktuální. Hlavním cílem GDPR je zajistit „ochranu fyzických osob v souvislosti se zpracováním osobních údajů a jejich volným pohybem". Účel shromažďování a uchovávání údajů má být omezen a jasně definován a osobní údaje je nutno zpracovávat po konkrétním souhlasu (čl. 6, odst. 4). Definice osobních údajů v nařízení GDPR zahrnuje všechny údaje týkající se zdravotního stavu daného jedince, takže zahrnuje i údaje sbírané CIED a přenesené systémy RM.

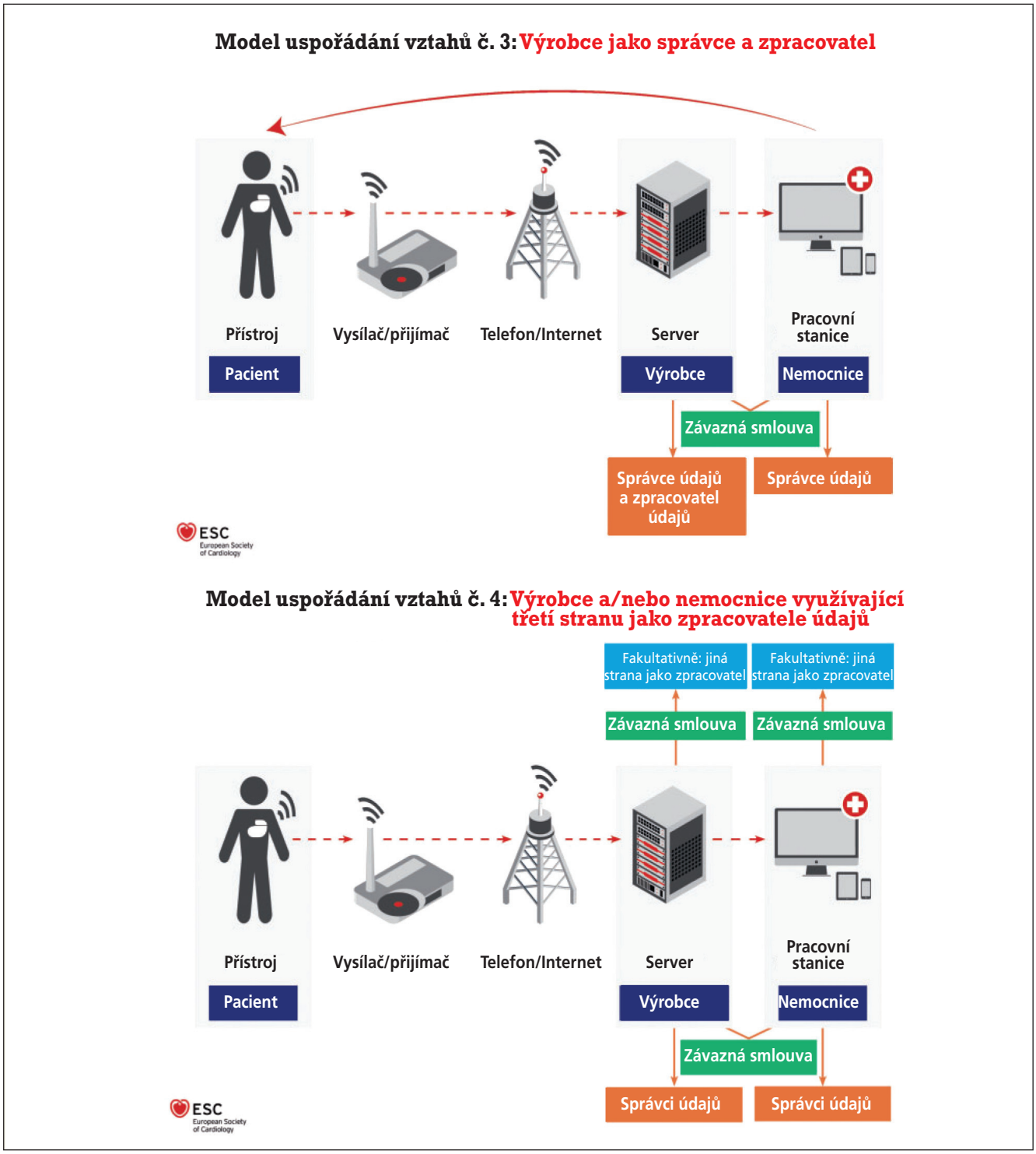
Klíčovým principem ustanoveným touto legislativou je, že jedinci i organizace shromažďující a uchovávající údaje musejí nést právní odpovědnost. Specifická právní odpovědnost je vymezena pro „správce údajů" (data controller), definovaného jako osoba nebo orgán, stanovující účely a způsoby zpracování osobních údajů, a pro „zpracovatele údajů" (data processor), definovaného jako osoba nebo orgán zpracovávající osobní údaje jménem správce a v souladu se všemi omezeními stanovenými správcem (čl. 4). V nařízení GDPR se konstatuje, že může existovat více než jeden správce, a znovu potvrzuje koncept společných správců, podle níž dva nebo více správců společně stanovují účely a způsoby zpracování údajů. V případě společných správců (čl. 26) nebo v případě správce a zpracovatele (čl. 28) musejí být stanoveny jejich podíly na odpovědnosti za dodržování nařízení GDPR, protože v případě jakéhokoli porušení budou muset obě strany obhájit svoji odpovědnost. Nařízení GDPR se nezabývá sdílením údajů mezi nezávislými správci a ve většině případů jsou tyto vztahy vymezeny formou smlouvy. V případě neplnění jejich odpovědností lze správcům nebo zpracovatelům údajů uložit významný finanční postih.

Používání osobních údajů

Jedinci mají zaručeno právo obdržet informace od správce údajů ohledně povahy a použití uchovávaných údajů a mají právo přístupu k vlastním údajům. S jistými výjimkami (například, kdy musí být chráněna bezpečnost státu) mají právo být zapomenuti a nechat si vymazat svoje údaje z konkrétní databáze (čl. 17). V obecné rovině mají



Obr. 1 – Obrázek znázorňuje tok údajů při RM CIED. Údaje jsou automaticky přenášeny **vysílačem/přijímačem (transceiverem) a sítí mobilních telefonů k zajištění serverů, které jsou u každého výrobce odlišné. Údaje jsou filtrovány a vystaveny na specifických webových st**ránkách nemocnice nebo výrobce; v případě potřeby může nemocnice kontaktovat pacienta **(horní šipka). Z právního hlediska je *správce údajů* (*data controller*) definován jako osoba nebo orgán určující účely a způsoby zpracování osobních údajů a *zpracovatel údajů* (*data processor*) jako osoba nebo orgán zpracovávající osobní údaje jménem správce a v souladu se všemi omezeními stanovenými správcem. Jak nemocnice, tak výrobci mohou používat poskytovatele třetí strany pro správu údajů, případně jejich analýzu pro konkrétní účely. Nemocnice a výrobci jsou běžně považováni za správce údajů, zatímco poskytovatelé třetí strany jsou běžně považováni za zpracovatele údajů (oranžová políčka). Pro všechny vztahy správce–správce a správce–zpracovatel je nutno vypracovat formální a transparentní smlouvu (zelená políčka) vymezující odpovědnosti a povinnosti každé ze stran ve vztahu ke shromažďování individuálních údajů a nakládání s nimi. Možnosti 1–4 popisují různé vztahy správce–správce a správce–zpracovatel. Uspořádání č. 3 zobrazuje situaci, kdy výrobce vystupuje jako zpracovatel údajů pro nemocnici (která v tomto vztahu vystupuje jako správce údajů), ale kdy je považován i za správce údajů při analýze údajů pro jiné účely než ty určené nemocnicí.** CIED (cardiac implantable electronic devices) – (aktivní) implantabilní elektronické přístroje v kardiologii; RM (remote monitoring) – dálková monitorace.



Obr. 1 – Pokračování

jedinci rovněž právo na „přenositelnost údajů“, což znamená, že mohou obdržet své osobní údaje ve „strukturovaném, běžně používaném a strojově čitelném formátu“, což jim umožní předat tyto údaje jinému správci, aniž by tomu původní správce bránil (čl. 20).

V jedné z preambulí k GDPR (bod odůvodnění 33) se uznává, že v době sběru dat je často nemožné popsat všechny účely, pro něž mohou tato data být zpracována v rámci vědeckého výzkumu. V takových případech proto mohou jedinci udělit souhlas s využitím svých údajů v určitých oblastech vědeckého výzkumu, a to za předpokladu dodržování uznávaných etických norem.

V článku 5 se uvádí, že další zpracování osobních údajů pro vědecké nebo statistické účely je možné. Článek 6, odst. 1, písm. c uvádí, že zpracování je zákonné, pokud je nezbytné pro splnění právní povinnosti, která se na správce vztahuje. Podle Evropského sboru pro ochranu osobních údajů (názor 3/2019, body odůvodnění 12 a 13) může

toto poskytnout právní základ pro zpracování osobních údajů v kontextu podávání zpráv o bezpečnosti; v kontextu inspekce příslušným národním úřadem; pro uchovávání údajů z klinických studií v souladu s povinností archivace stanovenou dokumentem EU Clinical Trials Regulation (regulace klinických studií v EU); nebo pro sponzora, případně investigátora pro splnění příslušných místních zákonů. Podle článku 6, písm. e je zpracování zákonné, pokud je nezbytné pro splnění úkolu prováděného ve veřejném zájmu.

Principy článku 6 se obecně týkají osobních údajů. Co se týče konkrétních kategorií, článek 9, odst. 2, písm. g uvádí, že zdravotní údaje lze zpracovávat v nezbytných případech z důvodů významného veřejného zájmu. Zdravotní údaje lze rovněž zpracovávat pro vědecký nebo historický výzkum nebo statistické účely v souladu s článkem 89, odst. 1 na základě práva Unie nebo členského státu (čl. 9, odst. 2, písm. j). I když je tedy zpracování osobních zdravotních údajů v zásadě zakázáno (čl. 9, odst. 1), existuje několik výjimek. Článek 9, odst. 2, písm. a umožňuje zpracování zdravotních údajů na základě výslovného souhlasu dotyčné osoby. Zpracování je rovněž povoleno, pokud je to nezbytné pro poskytování zdravotní péče nebo léčby nebo pro řízení zdravotnictví či sociálních systémů nebo služeb na základě práva EU nebo členského státu nebo na základě smlouvy se zdravotnickým pracovníkem. Konečně, zdravotní údaje lze rovněž zpracovávat z důvodů veřejného zdraví, jako je zajištění „přísných norem kvality a bezpečnosti zdravotní péče a léčivých přípravků nebo zdravotnických prostředků, na základě práva Unie nebo členského státu, které stanoví odpovídající a zvláštní opatření pro zajištění práv a svobod subjektu údajů, zejména služebního tajemství“ (čl. 9, odst. 2, písm. i).

Z výše uvedeného vyplývá, že pro zpracování zdravotních údajů není výslovný souhlas vždy vyžadován, například v případech, kdy klinický personál nahlíží do zdravotní dokumentace nebo kontroluje jiné zdravotní údaje pacientů pro účely stanovení diagnózy nebo plánu léčby. Sem patří i výstupy z RM.

Právní poradenství

Pro tento přehled si pracovní skupina objednala a získala odborné právní poradenství ke konkrétnímu výkladu požadavků GDPR v kontextu informací z RM implantovaných elektronických zdravotnických přístrojů.

Jakákoli společnost stanovující způsoby a účely shromažďování osobních údajů je považována za správce údajů (čl. 29 Pracovní skupina, str. 21). Pro výrobce, kteří zřizují systémy pro CIED, „způsoby“ znamenají nejen technické prostředky používané ke shromažďování údajů, ale i výběr a formát údajů požadovaných pro účinné RM. Správce je odpovědný za umožnění přístupu ke shromážděným osobním údajům a musí nabídnout možnost je vymazat (čl. 29 Pracovní skupina, str. 15).

Lékaři, zdravotničtí pracovníci i nemocnice mohou plnit dvojí nebo nezávislou úlohu (obr. 1). Pro účely RM CIED jejich pacientů musí být zdravotnické zařízení nebo nemocnice vždy považovány za správce údajů. V některých případech to je společně s individuálním zdravotníkem, pokud je tento zdravotnický pracovník lékařem se samostatnou praxí, pracuje ve zdravotnickém zařízení a působí jako správce. Jinak přebírá nemocnice v roli správce právní zodpovědnost za personál, který zaměstnává. Zdravotnické zařízení nebo nemocnice musí s výrobcem uzavřít řádnou závaznou smlouvu (obr. 1), v níž se berou v úvahu specifická pravidla pro transfer osobních údajů mimo EU.

Odborníci na právo doporučili, aby vztah mezi zdravotnickým zařízením a výrobcem pro správu a ochranu údajů získaných formou RM CIED byl založen na principu společných správců údajů. Formální a transparentní ujednání o odpovědnostech a povinnostech každé ze stran, co se týče shromažďování údajů jedinců (čl. 26), by mělo zahrnovat detaily o tom, jakým způsobem se mohou jedinci dostat ke svým osobním údajům, jak je mohou pozměnit nebo požádat o jejich vymazání (čl. 13 a 14). Doporučený vztah mezi poskytovatelem telemonitorovacích služeb v roli třetí strany a nemocnicí nebo výrobcem (v roli správce) je zpracovatel údajů.

Výrobci CIED se rovněž musejí řídit příslušnými ustanoveními nařízení o zdravotnických prostředcích (Medical Devices Regulation, MDR), shrnutými v doplňkovém materiálu online (příloha S2). Testování každého CIED ještě před jeho uvedením na trh musí zahrnovat ověření správného fungování hardwaru a softwaru pro RM v klinické praxi. V nařízení GDPR se uvádí, že veškerý software musí chránit soukromí již svým samotným návrhem a továrním nastavením (čl. 25) a že u každého projektu je třeba provést analýzu rizik z hlediska ochrany údajů. Nařízení MDR požaduje po výrobcích, aby po uvedení přístroje na trh dále dohlíželi na jeho fungování, což v případě CIED znamená shromažďování a analyzování údajů o technických aspektech fungování přístrojů při RM. Může se zdát, že toto ustanovení není – podle GDPR – slučitelné s právem jedince požadovat výmaz jejich osobních informací z databáze, žádný problém by však nevyvstal, pokud by výrobci uchovávali pouze anonymizované nebo pseudonymizované údaje (viz čl. 4, odst. 5 GDPR). Otázky spojené s právními aspekty výše uvedeného jsou podrobněji rozbírány jinde.

Současný stav dálkového monitorování v Evropě

Pohled pacientů

Literatury o zkušenostech s RM, uváděných samotnými pacienty, je málo. V roce 2012 bylo podle jedné zprávy 95 % ze 385 pacientů s ICD ve Skandinávii „spokojeno“ nebo „velmi spokojeno“ s RM. Ústně popisované přínosy zahrnovaly pocit většího bezpečí, případně lepší péči, protože nepřetržitá monitorace přináší pacientům více „klidu na duši“ i možnost přenosu údajů v případě, kdy se necítili dobře nebo prodělali příhodu. Studie REMOTE-CIED s 300 evropskými pacienty se srdečním selháním, u nichž byl použit ICD, rovněž nalezla vysokou míru spokojenosti. Pacienti žijící v odlehlých oblastech oceňovali zvláště menší počet návštěv v rámci kontroly svého zdravotního stavu v nemocnici nebo ordinaci lékaře. Přesto se u 53 % pacientů objevily problémy jako nemožnost odeslání údajů a 19 % z 221 pacientů dotázaných, čemu by dávali přednost při dalším sledování, uvedlo, že si přejí v rámci kontroly svého zdravotního stavu pokračovat v osobních návštěvách příslušných klinik nemocnic.

V průzkumu Evropské komise provedeném v roce 2015 se na obecný dotaz o možnostech konzultace na téma

mobilního zdraví (mobile health, m-Health) vyskytl u 46 % z 211 odpovědí názor, že pro získání důvěry uživatelů jsou nezbytné nástroje důkladně zajišťující soukromí i zabezpečení údajů (jako jsou mechanismy jejich šifrování a autentizace uživatele). Polovina respondentů volala po zesíleném vymáhání ochrany údajů a pravidel platných pro přístroje pro tzv. m-Health. Další dotazování prokázalo velmi silnou podporu požadavku, aby veřejnost byla plně informována o tom, jak se využívají jejich údaje. Nicméně výrobci, třetí strany podílející se na RM, ani lékaři ve svých zprávách neuváděli, že by větší počty pacientů vyjadřovaly obavy či znepokojení ohledně ochrany údajů nebo kybernetické bezpečnosti. Zdá se rovněž, že ani skupiny hájící práva pacientů se těmito tématy pravidelně nezabývají, pokud se jim nedostává prostoru v médiích informujících o případném nelegálním napadání (hackingu) přístrojů.

Souhlas s RM se často získává od samotného pacienta poté, co mu byl implantován CIED a před jeho propuštěním z nemocnice, kdy se stále ještě nemusí cítit dobře, nebo může mít dokonce bolesti a jeho jediným cílem je jít domů a začít se zotavovat. Za těchto okolností mohou pacienti podepsat formulář souhlasu rychle, aniž by četli nebo dokonale porozuměli poskytnutým informacím. Optimální načasování pro získání tohoto souhlasu je teprve nutno zjistit, ale na základě rad od pacientů a shody mezi členy pracovní skupiny je pravděpodobně vhodnější souhlas získat spíše před implantací přístroje než po jeho implantaci. Pro případy, kdy to není možné (například pokud se přístroj implantuje v akutní situaci), musí mít klinika vypracovaný rutinní postup pro vysvětlení principu RM a získat informovaný souhlas po výkonu, během osobní návštěvy pacienta. Informace je nutno poskytnout v srozumitelném jazyce a formátu.

Zkušenost lékařů – výsledky průzkumu

V průzkumu, který provedla EHRA v roce 2014, uvedlo pouze 9 % lékařů, že jsou si vědomi právních aspektů RM CIED. Tato pracovní skupina provedla v roce 2019 další online průzkum vědomostí o RM CIED. Obdrželi jsme 320 odpovědí od elektrofyziologů (47 %), kardiologů (29 %), lékařů zabývajících se srdečním selháním (8 %) a techniků, zdravotních sester jejich kolegů (16 %) z 27 zemí, členů států ESC. Pracoviště s nízkým objemem výkonů (< 100 implantací CIED/rok), středně vysokým (100–500/rok) a vysokým (> 500/rok) zaslala 24 %, resp. 49 % a 27 % odpovědí.

V tomto novém průzkumu odpovědělo 49 % respondentů, že o nařízení GDPR vědí, aniž by nutně znali všechny důsledky tohoto nařízení pro RM CIED. Podle konkrétních definic GDPR se většina (58 %) respondentů označila za „správce" údajů, zatímco 42 % jich se označilo za „zpracovatele". Přibližně polovina (44 %) respondentů uvedla, že nařízení GDPR ovlivnilo jejich praxi v souvislosti s RM mírně nebo významně; jako konkrétní problémy uvedli logistiku (52 %) a zvýšené nároky na čas (50 %). Právní důsledky zmínila pouze 4 % respondentů.

Možné problémy v oblasti kybernetické bezpečnosti připustilo 61 % účastníků průzkumu, přičemž 38 % z nich podniklo konkrétní kroky pro zmírnění těchto obav v jejich instituci, včetně používání prostředků, jako jsou firewall (61 %), šifrování (39 %), nové místní předpisy (38 %), právní poradenství (36 %), ověřování dvou faktorů (33 %), případně revize jejich formulářů souhlasu (25 %). Co se týče pacientů, 92 % respondentů uvedlo, že jejich pacienti nikdy nebo pouze vzácně vyjadřují obavy ohledně bezpečnosti svých údajů při RM CIED nebo že se dotazovali na možnosti přístupu ke svým na dálku shromažďovaným údajům z jejich CIED.

Výše uvedená zjištění názorně ukazují na to, jak nutné je, aby tento **konsenzuální dokument přispěl k jednotnému výkladu nařízení GDPR.**

Názory výrobců a poskytovatelů jako třetí strany

Dotazník k nařízení GDPR a kybernetické bezpečnosti byl zaslán všem výrobcům CIED, které jsou dostupné na evropském trhu i některým poskytovatelům z třetí strany. Všichni oslovení poskytli informace, jež byly použity k vytvoření tabulek 1 a 2. Získané údaje prokázaly nejednotnost ve výkladu a provádění opatření v souvislosti s nařízením GDPR; výrobci přitom konstatovali, že nemocnice mají nejednotné požadavky na ochranu údajů.

Všech pět výrobců definovalo zdravotnické instituce jako správce údajů (tabulka 1). Většina výrobců se sídlem mimo EU uvedla, že oni sami se považují pouze za zpracovatele údajů. Dvě společnosti uvedly, že se považují i za správce údajů; ostatní výrobci zahrnuli mezi správce i lékaře. Tyto názory se liší od jistého obecného vodítka, připraveného pro Evropskou komisi, i od výsledků našich právních konzultací.

Všichni výrobci CIED uvádějí, že pro přenos údajů z vysílače/přijímače do serverů a nemocnic přijímají opatření k zajištění kybernetické bezpečnosti. Průběžně sledují bezpečnostní incidenty a používají metody k obraně před útoky typu „denial of service attack" (tedy znefunkčněním nebo znepřístupněním internetové služby). K ochraně serverů pro RM slouží i fyzická ochrana a další prostředky, jako jsou speciální přístupové karty a bezpečnostní kamery. Provádějí se nezávislé zkoušky narušení prostor a audity dostatečnosti a účinnosti těchto opatření a v případě potřeby se používají ke zdokonalování bezpečnostních systémů.

Třetí strany jako provozovatelé monitorovacích systémů a systémů podávajících zprávy, kteří byli kontaktováni pro náš průzkum, shromažďují údaje o RM od různých výrobců a zpracovávají je pro třídění varovných upozornění. Odpovědi na náš dotazník zaslalo pět společností (Fleischhacker®, Focuson®, Fysicon®, Implicity® a Lindacare®). Jejich systémy používají buď vlastní servery, nebo fungují zcela na hostitelském serveru s přístupem přes virtuální soukromé síťové připojení, případně využívají cloudového prostředí. Podobně jako u výrobců CIED existuje ve výsledcích průzkumu značná heterogenita (tabulka 2). Všichni poskytovatelé jako třetí strany považují zdravotnické instituce, případně lékaře za správce údajů (a tedy sebe automaticky za zpracovatele údajů). Uváděná opatření v oblasti kybernetické bezpečnosti jsou srovnatelná s těmi přijatými výrobci CIED.

Hodnocení formulářů souhlasu

Nařízení GDPR uvádí, že jakákoliv osoba, která poskytne své osobní údaje ke sdílení („subjekt údajů"), by měla do-

Tabulka 1 – Průzkum u výrobců CIED ohledně dodržování zásad nařízení GDPR

Otázka	Abbott	Biotronik	Boston Scientific	Medtronic	Microport
Přístup zaměstnanců k PPD					
Jak je přístup k PPD interně kontrolován?	Přístup mají pouze zaměstnanci, kteří to potřebují pro výkon svého povolání, v souladu s platnými zákony. Odpovídající technická a organizační opatření.	Přístup k PPD je kontrolován na principu autorizace (oprávnění). Přístup k PPD mají pouze zaměstnanci, kteří jej potřebují podle principu „potřebuji vědět" (need to know). Pro kontrolu přístupu jsou zavedena technická a organizační opatření.	Dvoustupňová (two-factor) autentizace. Kontrola přístupu podle pracovního zařazení. Školení a postupy týkající se zabezpečení údajů.	Přístup pro osoby, které ho potřebují pro výkon svého povolání na principu nezbytného minima. Zavedena jsou kontrolní opatření jako prevence proti náhodnému a nezákonnému zničení, ztrátě, pozměňování, neoprávněnému zveřejnění a dalším nezákonným formám zpracování.	K PPD nemá přístup nikdo s výjimkou osob na lince technické podpory (helpdesk) s kvalifikací pro podporu pacientů v zasílání a instalaci domácího monitoru. Pracovníci linky technické podpory mají přístup k údajům pouze v režimu čtení.
Musejí zaměstnanci s přístupem k PPD absolvovat znalostní testy nebo certifikace pro dodržování zásad nařízení GDPR?	Ano, zaměstnanci absolvují školení k dodržování zásad GDPR a dalších zákonů týkajících se respektování soukromí ochrany údajů.	Pořádají se pravidelná školení a kursy na téma ochrany údajů a zaměstnanci jsou zavázáni k zachovávání tajemství.	Ano, zaměstnanci absolvují školení na téma požadavků ochrany údajů obecně a konkrétně nařízení GDPR.	Ano, provádí se povinné interní školení a znalostní testy obecně na téma zásad a postupů podle nařízení GDPR. Navíc se provádí konkrétní školení k nedávno aktualizované smlouvě o speciální síti CareLink.	Zaměstnanci linky technické podpory absolvují před zpřístupněním systému testy týkající se dálkového monitorování. Zahajují se školicí kursy zahrnující znalostní testy.
Regulační aspekty					
Považuje vaše společnost sériové číslo hardwaru za součást PPD?	Ano	Ano	Ano	Ano	Ano, v případech, kdy je možné spojit je přímo nebo nepřímo se subjektem údajů nebo odvodit informace o subjektu údajů či dedukcí.
Ve které zemi/zemích jsou umístěny servery uchovávající chráněné osobní údaje z vašich evropských RMS?	USA	Evropa	Irsko a USA	Nizozemsko	Francie
Kdo je vlastníkem PPD shromážděných z vašich evropských RMS?	V Evropě neexistuje pojem vlastnictví osobních údajů.	Pacient	Podle zákonů se může vlastnictví lišit od země k zemi na základě jurisprudence – obecně PPD patří subjektu údajů.	V Evropě neexistuje pojem vlastnictví osobních údajů.	Správce údajů (tzn. HCP)
Koho považujete za správce údajů z vašeho RMS?	□ Lékaře ■ Zdravotnické zařízení ■ Naši společnost	□ Lékaře ■ Zdravotnické zařízení □ Naši společnost	□ Lékaře ■ Zdravotnické zařízení ■ Naši společnost	□ Lékaře ■ Zdravotnické zařízení □ Naši společnost	■ Lékaře ■ Zdravotnické zařízení □ Naši společnost

Pokračování na další straně

Tabulka 1 – Průzkum u výrobců CIED ohledně dodržování zásad nařízení GDPR *(Dokončení)*

Otázka	Abbott	Biotronik	Boston Scientific	Medtronic	Microport
Přístup zaměstnanců k PPD					
Spolupracuje vaše společnost se třetími stranami, které přenášejí, používají, uchovávají nebo mají přístup k PPD vašeho RMS?	Ano. Místní přidružené společnosti v případech, kdy musejí poskytovat zákaznickou podporu, a další přidružené společnosti pro technickou podporu.	Ano Pobočky pro přístup k určitým údajům pro zákaznickou podporu a dodatečné služby.	Ano IT podpora (odstraňování problémů, technická pomoc, údržba)	Ano Speciální služba FocusOn, pokud mají smlouvu s HCP.	Ne
Žádá vaše společnost pacienty, aby podepsali informovaný souhlas umožňující vaší společnosti shromažďovat PPD z vašeho RMS?	Ano	Ne To je odpovědnost správce.	Ano	Ne Za získávání informovaného souhlasu od pacientů je odpovědná klinika nebo nemocnice.	Ne Microport poskytuje HCP návrh informovaného souhlasu pacienta.
Shromažďuje a uchovává vaše společnost místo pobytu pacienta?	Ne	Ne	Ne	Ne	Ne
Dopady nařízení GDPR					
Kolik pacientů kontaktovalo vaši společnost s otázkami ohledně nařízení GDPR?	Nepatrný počet	Žádný	< 10 pacientů	Medtronic je pouze zpracovatelem údajů. Medtronic běžně žádá pacienty, aby se obraceli na své zdravotnické zařízení.	Žádný
Jaký dopad má nařízení GDPR na fungování vašeho RMS?	Téměř žádný	Téměř žádný	Poměrně malý Sledování souhlasu pacienta. Obnova smluv na zpracování údajů s nemocnicemi a aktualizace formulářů souhlasu.	Téměř žádný	Téměř žádný Dokumentování zpracování údajů (v registru činností zpracování). GAP analýza současných opatření. Aktualizace informačních upozornění. Školicí kursy.
Uveďte prosím, do jaké míry ovlivnilo nařízení GDPR vaše podávání zpráv o fungování výrobku	Nijak	Nijak významně	Nijak	Poměrně málo	Nijak
Uveďte prosím, do jaké míry ovlivnilo nařízení GDPR analýzu obchodní činnosti vaší společnosti	Málo	Poměrně málo	Nijak	Málo	Nijak
Uveďte prosím, do jaké míry ovlivnilo nařízení GDPR váš vědecký výzkum	Málo	Poměrně málo	Málo	Poměrně málo	Nijak
Zhodnoťte prosím, do jaké míry ovlivnilo nařízení GDPR každodenní fungování vaší společnosti	Málo	Poměrně málo	Poměrně málo	Málo	Nijak

GDPR (General Data Protection Regulation) – obecné nařízení o ochraně údajů; HCP (healthcare provider) – poskytovatel zdravotní péče; PPD (private patient data) – osobní údaje pacienta; RMS (remote monitoring system) – systém dálkového monitorování.

Tabulka 2 – Průzkum poskytovatelů dálkového monitorování CIED jako třetích stran

Otázka	
Přístup zaměstnanců k PPD	
Jak je přístup k PPD interně kontrolován?	*Patentově chráněný server* (3): • Proces pro vytvoření identifikace uživatele, 24/7 audit a monitorování • Pro každý nový přístup k PPD je třeba vyplnit formulář, který musí schválit člen výkonného managementu společnosti, aby bylo možno vystopovat přístup a omezený čas/rozsah. • Přístup mají pouze oprávněné osoby. PPD jdou uloženy na zabezpečených místech, kam je k přístupu nutné konkrétní oprávnění.
	Služba VPN (2): • Všechny údaje jsou uloženy na serveru HCP, který odpovídá za umožnění přístupu společnosti a zaměstnancům ke své síti a informacím. K jedinému kontaktu s PPD by mohlo dojít během obsluhy a údržby prováděných na místě nebo přes dálkové přihlášení (log in) k serveru HCP.
Musejí zaměstnanci s přístupem k PPD absolvovat znalostní testy a získat osvědčení o znalosti nařízení GDPR?	• Pouze školení (2) • Testy (3) • Musejí rovněž podepsat chartu IT/závazek (1)
Kybernetická bezpečnost	
Jak je kontrolován přístup k PPD uchovávaným na serverech?	• VPN zákazníkova serveru (2) • VPN serveru společnosti v cloudovém prostředí (1) • Server společnosti s 24/7 auditem a monitorováním, splňující podmínky SOC2 (1) • VPN serveru společnosti NEBO server společnosti v cloudovém prostředí (1)
Zatrhněte prosím zavedená opatření k *ochraně* vašeho systému dálkového monitorování před nechtěným zveřejněním PPD	Šifrování (3) Dvoustupňová autentizace (2, ve vývoji 1) Firewall (3) Použití zařízení pro vyvažování zátěže (2) Detekce DDoS (3, a podle bezpečnostních opatření Microsoft Azure 1) Jiné: testy zranitelnosti (1) Nelze aplikovat (server zákazníka): 2
Došlo někdy ke kybernetickému útoku (příp. přibližně kolikrát)?	• Ne (3) • Žádný významný útok (kromě tisícovek DDoS běžných na systémech v cloudovém prostředí) (1) • Nelze aplikovat (1)
Byla kybernetická bezpečnost vašeho dálkového monitorovacího systému umístěného v Evropě někdy *narušena*?	Ne (4) Nelze aplikovat; jde o odpovědnost zákazníka
Regulační otázky	
Považuje vaše společnost *sériová čísla hardwaru* za PPD?	Ano (2) Ne (2) Nelze aplikovat; jde o odpovědnost zákazníka (zdravotnické instituce/nemocnice)
Ve které *zemi/zemích* jsou umístěny *servery* uchovávající PPD z vašich dálkových monitorovacích systémů v Evropě?	Nelze aplikovat (2) Francie (2) Spojené království pro tamní zákazníky (1) AWS cloud ve Frankfurtu, Německo (1) PC pro dálkovou podporu přístupu do serveru HCP jsou umístěny v Německu (1)
Kdo *je vlastníkem PPD* shromážděných z vašich dálkových monitorovacích systémů umístěných v Evropě?	Shromážděné PPD jsou majetkem pacientů, avšak lékaři používající platformu jsou považováni za správce. Nemocnice
Koho považuje vaše společnost za *správce údajů* PPD shromážděných z vašeho dálkového monitorovacího systému?	Pouze lékaře (1) Lékaře + zdravotnickou instituci (1) Zdravotnickou instituci (1) Nelze aplikovat; jde o odpovědnost zákazníka (zdravotnické instituce/nemocnice) (2)
Žádá vaše společnost pacienty *o podepsání informovaného souhlasu*, což by vaší společnosti umožnilo shromažďovat PPD z vašich systémů dálkového monitorování? Pokud ano, můžete nám jej laskavě poskytnout?	Ano (1) Ne (3): za získávání informovaného souhlasu pacienta odpovídá klinika nebo nemocnice Zatím ne, ale pracuje se na tom (1)

Pokračování na další straně

Tabulka 2 – Průzkum poskytovatelů dálkového monitorování CIED jako třetích stran *(Dokončení)*	
Otázka	
Shromažďuje a uchovává vaše společnost místo pobytu pacientů?	Ano (1) Ne (4)
Důsledky nařízení GDPR	
Pokud je vám známo, kolik pacientů se obrátilo na vaši společnost s dotazy souvisejícími s nařízením GDPR?	Žádný (5)
Uveďte prosím, do jaké míry ovlivnilo nařízení GDPR *fungování vaší platformy dálkového monitorování*. Jak?	Nijak (2) Poměrně málo (3). Pro dodržování pravidel nařízení GDPR bylo nutno vyvinout několik opatření/funkcionalit navíc.
Uveďte prosím, do jaké míry ovlivnilo nařízení GDPR *analýzu obchodní činnosti vaší společnosti.* Jak?	Nijak (2) Málo (1) Poměrně málo (2)
Zhodnoťte prosím, do jaké míry ovlivnilo nařízení GDPR *každodenní fungování vaší společnosti*.	Nijak (1) Málo (1) Poměrně málo (2). Pro dodržování pravidel nařízení GDPR byly vypracovány nová firemní taktika a postupy. Nařízení GDPR se projevilo i v oblasti interní IT. Významně (0) Zásadním způsobem (1)

DDoS (distributed denial of service) – útok DoS (znefunkčnění nebo znepřístupnění internetové služby); GDPR (General Data Protection Regulation) – obecné nařízení o ochraně údajů; HCP (healthcare provider) – poskytovatel zdravotní péče; IT (information technology) – informační technologie; PC (personal computer) – osobní počítač; PPD (private patient data) – soukromé údaje pacienta; SOC2 (Service Organization Control 2) – audit SOC2; SSL (Secure Sockets Layer) – protokol SSL; VPN (virtual private network) – virtuální soukromá síť. Počty odpovědí jsou uvedeny v závorkách.

stat dostatečné a srozumitelné informace ohledně druhu sdílených individuálních údajů i názvu příjemců (čl. 13, odst. 1, písm. e). V Evropě je ve většině institucí běžnou praxí, že získávají informovaný souhlas s RM spíše vyplněním formulářů připravených a poskytovaných výrobci než vyplněním formulářů připravených každou institucí. Souhlas musí získat správce údajů: může jej získat jeden správce i jménem společného správce (nebo jiného nezávislého správce), pokud se tato skutečnost jednoznačně sdělí subjektu údajů, a když je uvedený výkon přesně popsán v ujednání mezi správci.

Provedli jsme hodnocení formulářů informovaného souhlasu pěti výrobců CIED, které byly distribuovány kardiology a nemocnicemi během ledna a února 2019. Členové pracovní skupiny poskytli formuláře používané v jejich vlastních institucích a zemích; formuláře z jiných zemí byly získány s pomocí členů jejich národních kardiologických společností. Celkem bylo získáno 72 informačních listů a formulářů souhlasu používaných v 16 evropských zemích; tyto dokumenty byly systematicky analyzovány z hlediska 20 kritérií týkajících se RM a uchovávání údajů, partnerství, práv, přístupu k údajům, využívání údajů pro jiné účely, jejich anonymizace a právní odpovědnosti (tabulka 3). Shoda mezi zeměmi v textech každého výrobce byla posouzena srovnáním jejich verzí v různých jazycích.

Ve většině případů nebyly písemné informace poskytnuté ve formulářích souhlasu jasné, pokud se týče způsobu nakládání s údaji z RM. Jeden výrobce nedefinoval, kolik partnerů bude mít přístup k údajům, zatímco jiní výrobci uváděli různé počty. Strana odpovědná za údaje nebyla definována jedním výrobcem a ostatními výrobci označena současně jako lékař i nemocnice. Žádný výrobce nedefinoval jasně, kdo by měl být považován za „správce údajů"; konkrétní odpovědnost každého výrobce ve vztahu k údajům nebyla určena. Pokud se týče uchovávání údajů, žádné podrobnosti neposkytli dva výrobci. Ve formulářích čtyř výrobců nebyla práva pacientů jasně vysvětlena; podle dvou výrobců by pacienti neměli mít přístup k vlastním údajům ani možnost odvolat svůj souhlas.

Ve většině případů nebyla definována doba platnosti smlouvy; čtyři výrobci neuvedli, jak dlouho budou údaje pacientů uchovávány. Čtyři výrobci uvedli, že všechny údaje pro výzkum budou anonymizovány. Pouze jeden formulář popsal nějaká technická omezení RM. Nebyly poskytnuty žádné linky na webové stránky nebo zdroje dalších informací. Ve všech případech se informovaný souhlas u každé společnosti lišil mezi jednotlivými jazyky a zeměmi z hlediska struktury, čtivosti a obsahu. Jedna společnost například uvedla v informacích poskytovaných v jedné zemi a jazyku, kde budou uchovávány údaje pacientů, stejnou informaci ve svých formulářích používaných v jiných zemích však již neposkytla.

Tato analýza dokumentů ze 16 zemí nemusí odrážet situaci v celé Evropě. Do doby, než vstoupilo nařízení GDPR v platnost, musela každá země zavést vlastní postupy pro plnění požadavků předchozí direktivy EU. Je možné, že některé společnosti v té době stále revidovaly formuláře souhlasu a že některé nemocnice nezačlenily nejnovější verze do své každodenní praxe. Někteří poskytovatelé zdravotnických služeb možná po dohodě s každým výrobcem používají vlastní formuláře informovaného souhlasu. Někteří výrobci mohli své formuláře souhlasu od doby jejich hodnocení touto pracovní skupinou upravit.

Nevíme, do jaké míry čtivost formulářů souhlasu souvisí s průměrnou úrovní vzdělání a gramotností pacientů v každé zemi, ale většina formulářů souhlasu používá do jisté míry odborné termíny bez podrobných definic. Žádný z nich nepoužívá k vysvětlení principu RM nákresy nebo

Tabulka 3 – Hodnocení formulářů souhlasu k dálkovým monitorováním CIED

	Abbott	Biotronik	Boston Scientific	Medtronic	Microport
Jasná definice dálkového monitorování	Několik aspektů není jasných	Většina aspektů je jasně definována	Většina aspektů je jasně definována	Některé aspekty nejsou dobře definovány	Řada aspektů není definována
Jasné vysvětlení, jak se bude s údaji nakládat	Ne	Ne	Ano	Ne	Ne
Počty partnerů	Praktický lékař, nemocnice, společnost a partneři	Praktický lékař, servisní partneři	Praktický lékař, nemocnice, společnost a partneři	Pacient, praktický lékař, nemocnice a třetí strana	Není definováno
Doba platnosti smlouvy	Není definováno	Není definováno	Šest let po odpojení	Není definováno	Není definováno
Kdo je odpovědný za údaje?	Lékař, nemocnice	Lékař	Nemocnice/klinika	Není definováno	Nemocnice
Kdo je odpovědný za osobní údaje?	Lékař, nemocnice	Lékař	Nemocnice/klinika	Zdravotnické zařízení	Nemocnice
Kdo bude mít přístup k údajům?	Společnost, třetí strana, praktický lékař a nemocnice	Není definováno	Společnost, subdodavatelé, praktický lékař a další lékaři, kteří udělí právo přístupu, vaše nemocnice, zdravotnické orgány	Společnost, třetí strana. Úlohy praktického lékaře a nemocnice nejsou definovány.	Praktický lékař, nemocnice, společnost a pacient
Budou se údaje uchovávat mimo nemocnici?	Ano, v USA	Není definováno	Ano	Ano	Není definováno
Kdo bude uchovávat údaje?	Společnost	Není definováno	Společnost a subdodavatelé	Společnost a třetí strana	Není definováno
Jsou práva pacientů jasně vysvětlena?	Ne	Ne	Ano	Ne	Ne
Má pacient přístup k údajům a/nebo může odvolat souhlas? Je tato otázka jednoznačně definována?	Ne. I pokud pacient odvolá souhlas, jeho údaje se budou používat po dobu deseti let.	Ano, avšak postup není definován	Ano	Ano, napsáním dopisu lékaři	Ano
Budou údaje použity pro statistické nebo výzkumné účely?	Ano	Medicínsko-technický výzkum	Ano, po předchozí anonymizaci	Ano	Není definováno
Je vymezena odpovědnost každé strany (správa údajů, údržba databáze, získaných údajů, softwaru)?	Ne	Ne	Ne	Ne	Ne
Jsou jasně vymezeny údaje, které se budou získávat z kliniky, přístroje, osobního kontaktu s pacientem?	Ne	Ne	Ano	Ano	Ne

Pokračování na další straně

Tabulka 3 – Hodnocení formulářů souhlasu k dálkovým monitorováním CIED *(Dokončení)*

	Abbott	Biotronik	Boston Scientific	Medtronic	Microport
Přístup k údajům je jasně definován a oprávněný	Společnost, třetí strana, praktický lékař a nemocnice	Medicínsko-technický výzkum	Společnost, subdodavatelé, praktický lékař nebo jiný lékař, který umožní přístup, vaše nemocnice, zdravotnické orgány	Ano	Ne
Jak dlouho bude společnost uchovávat údaje	Není definováno	Není definováno	Alespoň šest let nebo více po skončení služby	Není definováno	Není definováno
Kde se budou údaje uchovávat (EU)?	USA	Není definováno	Irsko a USA	Daná země, Nizozemsko a USA	Není definováno
Pacient má různé možnosti volby ohledně informovaného souhlasu	Ne	Ne	Ano, (i) údaje pacienta, (ii) zdravotní údaje a (iii) statistické účely a výzkum	Ne	Ne
V případě výzkumných účelů budou údaje anonymizovány	Ano	Ano	Ano	Ano	Není definováno
Právo odvolat informovaný souhlas	Ano	Není definováno	Kontaktovat společnost, poslat e-mail nebo dopis společnosti nebo vaší nemocnici	Ano	Pouze identifikační údaje, nedefinované zdravotní údaje
Definice doby analyzování údajů	Ne, pouze v případě odvolání souhlasu	Ano, v pracovní době praktického lékaře	Ne	Ne	Není definováno
Přínos definován	Ano	Ano, pouze optimalizace vaší léčby	Ano	Ano	Není jednoznačně definováno
Stanovení technických omezení dálkového monitorování	Ne	Pouze omezení v souvislosti s telefonními sítěmi	Ne	Ne	Ne
V případě potřeby dalších informací, je uvedena nějaká webová adresa nebo jiný odkaz?	Ne	Ne, kontaktovat praktického lékaře	Ne	Ne	Ne
Popis omezení systémů	Ne	Telekomunikační systémy mobilního telefonu	Ne	Ne	Ne
Jsou formuláře informovaného souhlasu pro různé země shodné?	Ne	Ne	Ne	Ne	Ne

CIED (cardiac implantable electronic device) – implantabilní elektronický přístroj v kardiologii.
Byly hodnoceny formuláře souhlasu pěti výrobců CIED, které jsme v lednu a únoru 2019 obdrželi od kardiologů a výrobců.

obrázky. V některých formulářích jsou hustě psané pasáže s malým písmem, jež jsou pro řadu starších pacientů, kteří potřebují CIED, nejspíše obtížně čitelné; objevili jsme i font o výšce pět (1 mm); jednalo se o text jedné společnosti, avšak pouze ve verzích formuláře použitých ve vybraných zemích. Pokud jsou tyto problémy běžné a pacienti rozumějí tomu, co mají podepsat pouze v omezené míře, lze namítat, že jejich podpis je neplatný.

Pro vypracování obecného informačního listu a vzorového formuláře souhlasu s RM použila tato pracovní skupina rady od pacientů s CIED.

Kybernetická bezpečnost a dálkové monitorování srdečních implantabilních elektronických přístrojů

S tím, jak se vyvíjely implantabilní zdravotnické přístroje, zmenšovali výrobci jejich rozměry a snižovali hmotnost. Dnes závisí fungování těchto přístrojů téměř výlučně na softwaru a jsou čím dále více navzájem propojené. I když není kybernetická bezpečnost hlavním tématem této zprávy, je třeba, aby lékaři měli alespoň základní povědomí o hlavních aspektech RM, zvláště proto, že budou muset o této metodě hovořit se svými pacienty, od nichž budou potřebovat souhlas. Některé základní termíny ohledně kybernetické bezpečnosti osobních údajů jsou definovány v doplňkovém materiálu online, příloha S3. Dokument vypracovaný Koordinační skupinou pro zdravotnické prostředky („Medical Device Coordination Group Document“) Evropské komise poskytuje komplexní informace pro výrobce, aby mohli plnit přísné bezpečnostní požadavky při vývoji implantabilních zdravotnických prostředků.

Současné CIED obsahují rádiové rozhraní umožňující bezdrátovou komunikaci s externími programovacími zařízeními nebo základnami, což dovoluje telemetrický přenos údajů i neinvazivní reprogramování nastavení parametrů přístroje. To je sice velký přínos pro pacienty, avšak větší objem softwaru a počet rozhraní v CIED významně rozšiřují prostor pro kybernetický útok a vystavují CIED nových hrozbám. Nedávno publikované studie odborníků v oblasti bezpečnosti prokázaly, že k provádění útoků na implantované zdravotnické přístroje včetně CIED lze využít jak bezdrátové rozhraní, tak analogové rozhraní (senzory a software uvnitř CIED). V současnosti jsou nebezpečnější bezdrátové útoky, protože se snadněji provádějí, zatímco analogové útoky lze úspěšně provádět pouze ze vzdálenosti do 5 cm, a ještě za určitých podmínek, které lze v praxi obtížně splnit.

Pokud se týče bezdrátových útoků na CIED, objevilo se několik zpráv o závažných bezpečnostních slabinách patentovaných bezdrátových protokolů používaných externími přístroji pro komunikaci s CIED. Uvedené studie nabízejí praktické ukázky, jak lze těchto zranitelných míst využít v *in vitro*, nicméně realistických laboratorních experimentech. I když – pokud je nám známo – dosud nebyly provedeny žádné *in vivo* útoky na pacienty, mohli by útočníci snadno využít bezdrátového principu komunikace mezi pacientovým CIED a externími přístroji nejen k zachycení přenášených údajů, ale i k zasílání zlomyslných zpráv do pacientova CIED. Pro pacienty by takové útoky mohly mít závažné důsledky, protože by potenciálně mohly ohrozit jejich soukromí nebo změnit funkce přístrojů. Vzhledem k těmto informacím vydal v březnu 2019 americký Úřad pro kontrolu potravin a léčiv (Food and Drug Administration) bezpečnostní sdělení upozorňující uživatele na slabiny z hlediska kybernetické bezpečnosti, protože telemetrický protokol nepoužíval šifrování, autentizaci ani autorizaci.

Jedním důležitým poučením z publikovaných studií bylo zjištění, že výrobci CIED běžně spoléhají na utajování specifikací jejich bezdrátového přenosu jako na jediný prostředek zabezpečení. Pro tento (ne zcela bezpečný) přístup se používá označení „bezpečnost díky neznalosti“ („security through obscurity“), protože předpokládá, že útočníci bez přístupu ke specifikacím protokolu nebudou schopni zjistit, jak systém uvnitř funguje. Několik odborníků nicméně prokázalo, že obecně lze patentově chráněné protokoly prolomit bez přechozích znalostí, což znamená, že nejsou vůbec bezpečné. Jediným řešením je chránit údaje přenášené mezi pacientovým CIED a vnějším přístrojem pomocí kryptografie v kombinaci s dalšími opatřeními. Výrobci CIED mohou přejít od svých slabých, ne zcela bezpečných patentově chráněných protokolů k odolnějším bezpečnostním řešením, která byla dostatečně ověřena odborníky v otázkách bezpečnosti, a ta pak použít podle standardních postupů pro zajištění bezpečnosti.

Mezinárodní srovnání

Od roku 2015, kdy HRS publikovala svůj konsenzuální dokument, se dálkové monitorování stalo v USA standardem péče o pacienty s CIED. Mezi lety 2006 a 2010 bylo přibližně 50 % amerických pacientů s CIED obdařených možností RM touto metodou aktivně monitorováno, a tento podíl stále roste. Pokud se RM nepoužívá, je to spíše důsledkem místní praxe než kvůli charakteristikám jednotlivých pacientů.

Načasování spuštění RM a osvěty pacientů i poskytovatelů péče se mezi jednotlivými institucemi liší. Pacienti obvykle dostávají vysílač/přijímač v době propuštění z nemocnice po implantačním výkonu nebo při jejich první kontrolní návštěvě lékaře po operaci. Pacienti i jejich ošetřovatelé dostanou informace, aby pochopili přínosy a limitace RM, dokázali nastavit vysílač/přijímač, věděli, že jejich lékař nebo jiný zdravotnický pracovník je v případě zjištění významné abnormality bude kontaktovat i co od nich arytmologická služba očekává pro účinnou spolupráci. I když získání podepsaného informovaného souhlasu před zahájením RM není v USA povinné, připravila organizace HRS pro pacienty informační list, který mohou kliniky pro tyto účely používat.

Pokud se pacienti sami nedotážou na to, kam plynou jejich data, obvykle se údaje o výrobcích nebo dalších subjektech zapojených do shromažďování, přenášení nebo uchovávání jejich údajů neprobírají. V USA se poskytovatelé zdravotní péče a pacienti zaměřují především na účinnou implementaci RM a dosud nezaznamenali významnější obavy či znepokojení ohledně ochrany údajů generovaných CIED a dále sdílených přes internet. Existuje sice oficiální doporučení, ale výrobci ve svých souhrn-

ných informacích o přístrojích žádné podrobnosti o kybernetické bezpečnosti neuvádějí.

Zásady informovaného souhlasu

Jeden ze základních principů lékařské etiky, tedy respektování autonomie každého pacienta, je zakotven v nejnovější revidované verzi Ženevské deklarace Světové lékařské asociace. Pacientům se musí dostat co nejvíce informací, které si přejí mít nebo které potřebují, aby mohli přijímat informovaná rozhodnutí. Evropský inspektor ochrany údajů („European Data Protection Supervisor“) nedávno uvedl, že souhlas jako právní základ pro zpracování údajů podle GDPR „musí být dobrovolný, konkrétní, informovaný a jednoznačný“. Aby byl souhlas platný, musí být informace poskytnuty v jazyce, kterému mohou snadno porozumět pacienti bez medicínských nebo technických znalostí, a ve snadno čitelné podobě. Důkazy z jedné kardiologické studie ukázaly, že tomu tak často není, a naše vlastní analýza formulářů souhlasu prokázala podobné odchylky od optimální praxe.

V tomto ohledu nám jako vodítko mohou posloužit poznatky z behaviorálních věd. Aby se pacient mohl rozhodovat účinně a kvalitně, musí se na diskusi podílet lékař nebo jiný zdravotnický pracovník. Obecně platí, že účast pacienta na rozhodování vede k lepším klinickým výsledkům. Použití různých pomůcek pro pacientovo rozhodování může tlumit účinně pocity úzkosti a zlepšit odběr anamnestických údajů. Například pacienti podstupující katetrizaci srdce byli méně anxiózní a lépe informovaní, pokud byli randomizováni do skupiny, která obdržela informace s použitím obrázků.

Konkrétně v kontextu CIED by byl užitečný další výzkum s cílem zjistit, jak dobře pacienti rozumějí způsobu monitorování jejich přístrojů i přenosu, zpracování a ukládání údajů. Nedávno publikovaná studie prokázala, že pacientům se dostává méně informací, než by očekávali a chtěli získat. Jedním z modelů, který by mohl znamenat možnost zkvalitnění tohoto procesu, je model dynamického souhlasu, což znamená, že pacienti mohou udělovat souhlas s různými součástmi péče v různých fázích a v různých časových obdobích, dle vlastního uvážení a s přístupem k dodatečným informacím, pokud a kdy si to přejí; tento model je popisován jako vnímání pacientů spíše jako „partnerů“ než „subjektů“. Zajímavým příkladem v tomto směru je Finsko, kde pacienti mají přes internet zajištěn zcela bezpečný přístup ke všem svým zdravotním záznamům v databázi pacientů, a každý pacient musí souhlasit s tím, že jejich údaje mohou být sdíleny mezi různými zdravotnickými zařízeními. Podle principu lékařské etiky má mít pacient kontrolu nad vlastními údaji a poskytnout předpokládaný přístup k nim během konzultace s lékařem nebo jiným zdravotnickým pracovníkem, ale pro jiné účely pouze výslovně.

Doporučení

Pro poskytování zdravotní péče podle nejnovějších poznatků a dodržování aktuálního znění nařízení GDPR je nutná dokonalá znalost nejen technických funkcí, ale i regulačních zásad platných pro medicínské prostředky. Lékaři i poskytovatelé zdravotní péče si rovněž musejí být vědomi zranitelných míst i obecných strategií pro posílení kybernetické bezpečnosti.

Výrobci CIED nepotřebují a nemusejí ani chtít získávat personalizované údaje, musejí však shromažďovat údaje o fungování přístrojů. Proto se doporučuje, aby výrobci vždy shromažďovali a zpracovávali minimální nezbytný objem identifikovatelných údajů, a kdykoli je to možné, měli přístup pouze k pseudonymizovaným údajům, jež by bylo možné v případě potřeby vystopovat pomocí unikátního identifikačního kódu daného přístroje (unique device identification, UDI). Pro účely některých technických analýz plně postačí anonymizované údaje.

Z pohledu této pracovní skupiny je potřeba vypracovat konsenzuální doporučení pro to, jaké údaje je potřeba shromažďovat a sdílet. Evropská asociace srdečního rytmu spolupracuje s Heart Rhythm Society a s výrobci na vypracování slučitelných protokolů. Následující doporučení se týkají konkrétně požadavků GDPR Evropské unie, kybernetické bezpečnosti CIED a důsledků pro získávání informovaného souhlasu:

Interpretace a zavádění nařízení pro obecnou ochranu údajů (General Data Protection Regulation)

Výrobci jsou správci údajů, pokud stanovují cíle („účely“) RM svých přístrojů, pokud určují, které údaje je nutno shromažďovat, a pokud vyvíjejí metody („prostředky“) k získávání těchto údajů. Pokud analyzují a uchovávají shromážděné údaje, mohou vystupovat i jako zpracovatelé údajů. Vzhledem k jejich úloze při stanovování cílů a metod RM však nejsou pouhými zpracovateli údajů ve vztahu k nemocnicím.

Nemocnice jsou rovněž správci údajů, protože stanovují klinické indikace pro shromažďování údajů na dálku z CIED i podrobnosti výkonu a určují, které údaje jednotlivých pacientů se shromažďují a analyzují.

Pracovní skupina doporučuje, aby pouze nemocnice byly schopny převádět pseudonymizované údaje z přístroje na informace konkrétního pacienta. Lékaři a ostatní zdravotničtí pracovníci zaměstnaní v nemocnici kontrolují údaje poskytnuté výrobcem nebo poskytovatelem jako třetí stranou; mohou následně přijímat jakákoli indikovaná klinická rozhodnutí, mohou uchovávat údaje a mohou zahájit a provádět sekundární analýzy údajů.

Nejvhodnějším modelem je model dvou společných správců. K tomu je třeba uzavřít závaznou smlouvu mezi dvěma správci, v níž jsou přesně vymezeny jejich příslušné odpovědnosti a povinnosti. Koncept takové smlouvy je dostupný jako doplňkový materiál online, příloha S4.

Nezávislé kardiology, kteří působí jako osoby samostatně výdělečně činné, je nutno považovat za správce údajů, pokud mají soukromou praxi nebo pracují jako soukromí/nezávislí praktičtí lékaři v nemocnici.

Poskytovatelé třetí strany jsou zpracovatelé údajů, pokud byli správcem údajů pověřeni ke shromažďování, analýze a přenosu údajů získaných RM CIED. Je nutno vypracovat smlouvu mezi správcem a zpracovatelem; témata, která musejí být ve smlouvě zmíněna, jsou uvedena v doplňkovém materiálu online, příloha S5.

Je zapotřebí konkrétního doporučení Evropského sboru pro ochranu údajů (European Data Protection Board), které se týká zachování rovnováhy mezi požadavky nařízení GDPR (umožňující pacientům individuální kontrolu jejich vlastních údajů) a požadavky nařízení o zdravotnických prostředcích (MDR) (požadující od výrobců dohled nad jejich zdravotnickými prostředky spojenými s vysokým rizikem). Právní konzultace ze strany Evropské komise by mohly objasnit otázky týkající se používání osobních údajů ze zdravotních registrů a klinických databází pro sekundární výzkum. Podle předběžného názoru evropského inspektora ochrany údajů (European Data Protection Supervisor) pověřeného ochranou údajů a vědeckým výzkumem, který byl publikován v lednu 2020, je třeba dále pracovat na vytvoření kodexu praxe.

Kybernetická bezpečnost

Výrobci musejí vyvinout bezpečné šifrované protokoly pro komunikaci mezi implantovaným CIED a jeho lokáním vysílačem/přijímačem. Výrobci musejí obecně popsat, jaká bezpečnostní opatření přijímají.

Všechny údaje přenášené internetem nebo přes cloudové úložiště výrobcům, poskytovatelům třetí strany a nemocnicím musejí být rovněž šifrovány nebo jakýmkoli jiným způsobem zabezpečeny.

Evropská komise musí založit a podporovat práci odborné laboratoře pro provádění testů zranitelnosti zdravotnických prostředků aktivovaných přes internet, jak zní ustanovení nařízení o zdravotnických prostředcích EU.

Informovaný souhlas

(1) Pracovní skupina doporučuje získávat souhlas jak pro implantaci CIED, tak pro jeho následné RM současně; ideálně ještě před implantací přístroje. To by měla být odpovědnost nemocnice, která má uchovávat i kopie formuláře souhlasu.
(2) Pacientům je nutno poskytovat informace v jejich mateřském jazyce bez nadměrného používání odborných výrazů. Popis implantátu a jeho monitorování musí být snadno pochopitelný průměrně gramotným osobám. Grafické informace jsou srozumitelnější než velké plochy textu. Nesmějí se používat malé fonty.
(3) Informace poskytnuté pacientovi musejí zahrnovat způsob přenosu jejich údajů, způsob zabezpečení celého procesu a s kým a pro jaké účely jsou údaje sdíleny. Informace připravené výrobci pro pacienty v souhrnu bezpečnosti a fungování v klinické praxi (Summary of Safety and Clinical Performance), který bude nyní k dispozici pro všechny implantabilní zdravotnické prostředky spojené s vysokým rizikem včetně CIED, musí obsahovat podrobnosti o dálkovém monitorování.
(4) Leták s obecnými informacemi a vzorový formulář souhlasu je k dispozici v doplňkovém materiálu online, příloha S6. Ten lze upravit podle konkrétních místních požadavků nebo pro konkrétní přístroje a nové technické prostředky, vždy však bude důležité vysvětlit princip RM jednoduchým jazykem bez právní terminologie a poskytnout odpovědi na časté dotazy.
(5) Pacientům je nutno umožnit přístup k jejich vlastním údajům shromážděným pomocí RM. Výrobci musejí sami dohodnout s nemocnicemi, jak toto zajistit, snad pomocí společného portálu, který by bylo možno rovněž používat pro dynamický souhlas. Předběžný návrh Evropské datové strategie přiznává absenci nástrojů, které by umožnily jednotlivcům domáhat se svých práv podle GDPR, jako například „webových rozhraní pro požadování přístupu k osobním údajům“.

Doplňkový materiál: dostupný online v časopise Europace.

Literatura*

1. Nielsen JC, Kautzner J, Casado-Arroyo R, et al. Remote monitoring of cardiac implanted electronic devices: legal requirements and ethical principles – ESC Regulatory Affairs Committee/EHRA joint task force report. Europace 2020;22:1742–1758.

* Všechny další odkazy lze nalézt v původním fulltextovém dokumentu.