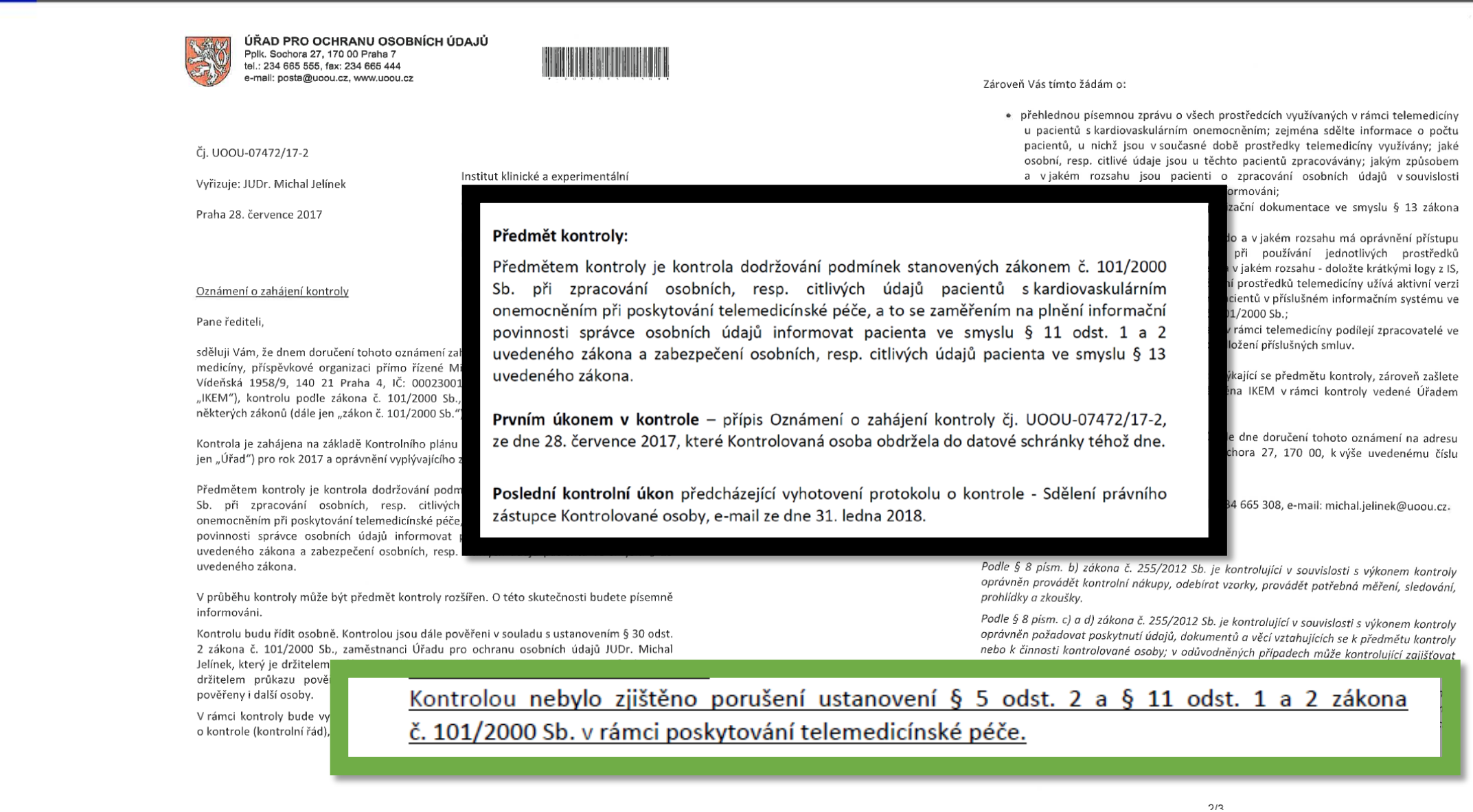
Ochrana osobních údajů při poskytování telemedicínské péče

Ing. Petr Raška – 25.04.2018

IK+E M

Úvod – aneb jak to začalo 1/2



ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ
Pplk. Sochora 27, 170 00 Praha 7
tel.: 234 665 555, fax: 234 665 444
e-mail: posta@uoou.cz, www.uoou.cz

Čj. UOOU-07472/17-2

Vyřizuje: JUDr. Michal Jelínek

Praha 28. července 2017

Institut klinické a experimentální

Oznámení o zahájení kontroly

Pane řediteli,

sděluji Vám, že dnem doručení tohoto oznámení zah
medicíny, příspěvkové organizaci přímo řízené Mi
Vídeňská 1958/9, 140 21 Praha 4, IČ: 00023001
„IKEM"), kontrolu podle zákona č. 101/2000 Sb.,
některých zákonů (dále jen „zákon č. 101/2000 Sb.")

Kontrola je zahájena na základě Kontrolního plánu
jen „Úřad") pro rok 2017 a oprávnění vyplývajícího z

Předmětem kontroly je kontrola dodržování podm
Sb. při zpracování osobních, resp. citlivých
onemocněním při poskytování telemedicínské péče,
povinnosti správce osobních údajů informovat p
uvedeného zákona a zabezpečení osobních, resp.
uvedeného zákona.

V průběhu kontroly může být předmět kontroly rozšířen. O této skutečnosti budete písemně informováni.

Kontrolu budu řídit osobně. Kontrolou jsou dále pověřeni v souladu s ustanovením § 30 odst. 2 zákona č. 101/2000 Sb., zaměstnanci Úřadu pro ochranu osobních údajů JUDr. Michal Jelínek, který je držitelem
držitelem průkazu pově
pověřeny i další osoby.

V rámci kontroly bude vy
o kontrole (kontrolní řád),

Předmět kontroly:

Předmětem kontroly je kontrola dodržování podmínek stanovených zákonem č. 101/2000 Sb. při zpracování osobních, resp. citlivých údajů pacientů s kardiovaskulárním onemocněním při poskytování telemedicínské péče, a to se zaměřením na plnění informační povinnosti správce osobních údajů informovat pacienta ve smyslu § 11 odst. 1 a 2 uvedeného zákona a zabezpečení osobních, resp. citlivých údajů pacienta ve smyslu § 13 uvedeného zákona.

Prvním úkonem v kontrole – přípis Oznámení o zahájení kontroly čj. UOOU-07472/17-2, ze dne 28. července 2017, které Kontrolovaná osoba obdržela do datové schránky téhož dne.

Poslední kontrolní úkon předcházející vyhotovení protokolu o kontrole - Sdělení právního zástupce Kontrolované osoby, e-mail ze dne 31. ledna 2018.

Zároveň Vás tímto žádám o:

- přehlednou písemnou zprávu o všech prostředcích využívaných v rámci telemedicíny u pacientů s kardiovaskulárním onemocněním; zejména sdělte informace o počtu pacientů, u nichž jsou v současné době prostředky telemedicíny využívány; jaké osobní, resp. citlivé údaje jsou u těchto pacientů zpracovávány; jakým způsobem a v jakém rozsahu jsou pacienti o zpracování osobních údajů v souvislosti
ormováni;
zační dokumentace ve smyslu § 13 zákona
do a v jakém rozsahu má oprávnění přístupu
při používání jednotlivých prostředků
v jakém rozsahu - doložte krátkými logy z IS,
ní prostředků telemedicíny užívá aktivní verzi
cientů v příslušném informačním systému ve
01/2000 Sb.;
v rámci telemedicíny podílejí zpracovatelé ve
ložení příslušných smluv.

ýkající se předmětu kontroly, zároveň zašlete
ena IKEM v rámci kontroly vedené Úřadem

e dne doručení tohoto oznámení na adresu
chora 27, 170 00, k výše uvedenému číslu

84 665 308, e-mail: michal.jelinek@uoou.cz.

Podle § 8 písm. b) zákona č. 255/2012 Sb. je kontrolující v souvislosti s výkonem kontroly oprávněn provádět kontrolní nákupy, odebírat vzorky, provádět potřebná měření, sledování, prohlídky a zkoušky.

Podle § 8 písm. c) a d) zákona č. 255/2012 Sb. je kontrolující v souvislosti s výkonem kontroly oprávněn požadovat poskytnutí údajů, dokumentů a věcí vztahujících se k předmětu kontroly nebo k činnosti kontrolované osoby; v odůvodněných případech může kontrolující zajišťovat

Kontrolou nebylo zjištěno porušení ustanovení § 5 odst. 2 a § 11 odst. 1 a 2 zákona č. 101/2000 Sb. v rámci poskytování telemedicínské péče.

2/3

Úvod – aneb jak to začalo 2/2

Přehled podkladů:

Protokol o kontrole se opírá o následující podklady (údaje, dokumenty a věci vztahující se k předmětu kontroly nebo k činnosti Kontrolované osoby a dokumenty, které byly pořízeny v průběhu kontroly), popř. o dokumenty a skutečnosti, které jsou kontrolnímu orgánu známy z jeho úřední činnosti.

1. Kontrolní plán pro rok 2017 ze dne 12. ledna 2017 (revize ke dni 28. června 2017), č.j. UOOU-07472/17-1;
2. Oznámení o zahájení kontroly ze dne 28. července 2017, č.j. UOOU-07472/17-2;
3. Poskytnuté podklady od IKEM ze dne 18. srpna 2017, č.j. UOOU-07472/17-3 + přílohy:
   - Průvodní dopis
   - Seznam příloh
   - Plná moc
   - Formulář Souhlas pacienta s používáním služby Biotronik Home Monitoring (cardioMessenger)
   - Formulář o zplnomocnění a souhlasu pacienta systém péče o pacienty Merlin.Net™
   - Služby CareLink- Souhlas pacienta s ohledem na ochranu údajů
   - Logy z IT systému
   - Organizační směrnice Povinná mlčenlivost pracovníků ve zdravotnictví
   - Organizační směrnice Zdravotnická dokumentace
   - Organizační směrnice Provozování informačních technologií a použití hardware a software v IKEM
   - Formulář Žádost o login a přístupy do systémů IKEM
   - Formulář Prohlášení o seznámení se základními bezpečnostními mechanismy pro ochranu informačních zdrojů IKEM
   - Znalecký posudek č. 151-5/2017 – Posouzení bezpečnosti využití elektronického podpisu v aplikaci pro recepty
   - Uživatelská smlouva systému péče o pacienty ST. JUDE MEDICAL Merlin.Net™
   - Systém péče o pacienty ST. JUDE MEDICAL Merlin. Net™ – Všeobecné smluvní podmínky
   - Formulář o zplnomocnění a souhlasu pacienta – Systém péče o pacienty Merlin. Net™
   - Registrace Úřad pro ochranu osobních údajů
   - Merlin.Net Patient Care Network Safe Harbor Certifikation FAQ
   - Privacy Shield St. Jude Medical
   - Bezpečnostní příručka Merlin.Net Patient Care Network (PCN) Otázky, odpovědi k systému Merlin.Net Patient Care NetworkNews Release (St. Jude Medical)
   - European union data processing and transfer policy (Politika Evropské unie pro zpracování a přenos dat)
   - Síťové služby Medtronic Carelink® – Všeobecné podmínky;
4. Žádost o součinnost ze dne 9. října 2017, č.j. UOOU-07472/17-4;
5. Žádost o změnu času konání ústního jednání a místního šetření ze dne 11. října 2017, č.j. UOOU-07472/17-5 (e-mail) + přílohy:
   - Substituční plná moc (Mgr. Matyáš Kužela)
   - Program konference;
6. Žádost o změnu času konání ústního jednání a místního šetření ze dne 11. října 2017, č.j. UOOU-07472/17-6 + přílohy (listinná podoba):
   - Substituční plná moc (Mgr. Matyáš Kužela)
   - Program konference;
7. Žádost o součinnost – vyrozumění ze dne 13. října 2017, č.j. UOOU-07472/17-7;
8. Záznam z ústního jednání a místního šetření konaného v IKEM dne 26. října 2017, č.j. UOOU-07472/17-9 + přílohy:
   - Poskytnutí dodatečných podkladů a informací
   - Substituční plná moc – kopie
   - Kopie zdravotnické dokumentace se záznamem dálkové kontroly (kardiostimulátoru/ICD přístroje) včetně souhlasu s poskytováním telemedicínské péče 3x (Biotronik, Medtronic, St. Jude Medical)
   - Seznam osob oprávněných v rámci telemedicínské péče
   - Žádost o login 2x
   - Pasportní list počítače (formulář)
   - Žádost o připojení soukromého zařízení k počítačové síti IKEM (formulář)
   - Prohlášení o seznámení se základnímu bezpečnostními mechanismy pro ochranu informačních zdrojů IKEM 2x;
9. Vyjádření IKEM k úřednímu záznamu o provedení kontrolního úkonu ze dne 13. listopadu 2017, č.j. UOOU-07472/17-11 + přílohy:
   - Printscreen ze systému Biotronik – 2x
   - Printscreen ze systému Medtronic – 2x
   - Printscreen ze systému St. Jude Medical – 1x
10. Úřední záznam o provedení kontrolního úkonu – oprava ze dne 16. listopadu 2017, č.j. UOOU-07472/17-12;
11. Úřední záznam o nahlédnutí do kontrolního spisu ze dne 19. prosince 2017, č.j. UOOU-07472/17-16;
12. Sdělení Kontrolované osoby, e-mail ze dne 23. ledna 2018, č.j. UOOU-07472/17-17
13. Odpověď na sdělení Kontrolované osoby, e-mail ze dne 23. ledna 2018, č.j. UOOU-07472/17-18;
14. Sdělení Kontrolované osoby, e-mail ze dne 30.. ledna 2018, č.j. UOOU-07472/17-19
15. Odpověď na sdělení Kontrolované osoby, e-mail ze dne 31. ledna 2018, č.j. UOOU-07472/17-20;
16. Sdělení Kontrolované osoby, e-mail, ze dne 31. ledna 2018, č.j. UOOU-07472/17-21
    - příloha Smlouva o zpracování osobních údajů uzavřená IKEM a Biotronik Praha, s.r.o.

Shrnutí – co jsme se naučili

- Poskytování péče telemedicínou zdravotnickým zařízením a příslušným poskytovatelem služeb zahrnuje zpracování určitého typu údajů o pacientovi.

- Toto zpracování spadá do oblasti působnosti nařízení o ochraně údajů. Navíc jsou zpracovaná data považována za citlivá a vyžadují zvýšenou ochranu.

- Pokud jde o údaje o telemedicíně, zdravotní zařízení by mělo být vždy považováno za správce údajů, který určuje účel a prostředky zpracování a nakonec je odpovědný.

- Na druhé straně může poskytovatel služeb telemedicíny jednat buď jako (a) zpracovatel zdravotnického zařízení nebo (b) nezávislý správce.
- Z pohledu zdravotnického zařízení je hlavní výhodou vztahu mezi správcem a zpracovatelem kontrola zdravotnického zařízení nad zpracovanými daty.
- Hlavní nevýhodou je odpovědnost za zpracování provedené zpracovatelem. Rovněž je nutné uzavřít písemnou dohodu o zpracování údajů mezi stranami.

- Ve scénáři správce vs správce není zdravotnické zařízení odpovědné za zpracování provedené poskytovatelem služeb. Zdravotní zařízení však nemá nad takovýmto zpracováním kontrolu.
- Dále je vyžadován souhlas pacienta s (a) předáváním osobních údajů poskytovateli a (b) zpracování, které je prováděno.
- Zpracování založené na souhlasu je obecně méně spolehlivé, jelikož subjekty údajů mohou odňat (nebo odmítnout udělit) svůj souhlas.
  Pokud jde o ochranu údajů, vzhledem k citlivé povaze zpracovávaných údajů se doporučují bezpečnostní opatření, jako jsou přístupová práva, protokoly, pseudonymizace a šifrování

Telemedicína

- Obecně platí, že péče v oblasti telemedicíny znamená používání informačních a komunikačních technologií ("ICT"), které umožňují nebo zlepšují přístup pacienta k lékařské péči v situacích, kdy zdravotnický personál a pacient nejsou na stejném místě.

- V případě kardiologické kliniky IKEM zahrnuje péče v oblasti telemedicíny zejména tzv. Telemonitoringové služby;
- tj. za použití implantovaných zařízení pro vzdálené shromažďování údajů týkajících se (a) zdravotního stavu pacienta a (b) implantovaného zařízení.
- To umožňuje IKEM přístup a vyhodnocení určitých údajů pacienta bez osobní návštěvy pacienta v IKEM.
- Telemedicína proto (mimo jiné) výrazně zlepšuje pohodlí a dostupnost pacienta.

- Pro poskytování péče o telemedicínu využívá kardiologická klinika IKEM přístroje vyráběné různými dodavateli (dále jen "dodavatelé").
- Každý dodavatel je rovněž odpovědný za (a) shromažďování a uchovávání údajů shromážděných prostřednictvím implantovaného zařízení a (b) umožnění přístupu k těmto údajům pracovníkům kliniky kardiologie IKEM.

Zpracování osobních údajů

- Informace týkající se určité fyzické osoby tvoří tzv. Osobní údaje podle zákona o ochraně osobních údajů a dne 25. května 2018 (dále jen "GDPR") vstoupí v platnost nové nařízení o obecném obecném ochraně údajů.
- Vzhledem k výše uvedeným zákonům o ochraně osobních údajů a od 25. května 2018 se GDPR vztahuje na zpracování údajů shromážděných prostřednictvím implantovaného zařízení a vztahujících se k určitému pacientovi.

- Kromě toho, jak potvrzuje DPA v rámci kontroly, zákon o ochraně osobních údajů a GDPR se vztahují i na zpracování, i když příslušný dodavatel nezná totožnost pacienta.
- Tento závěr DPA je založen na argumentu (podle našeho názoru správného), že i když dodavatel sám o sobě není schopen přiřadit shromážděná data konkrétnímu pacientovi, taková vazba mezi daty a příslušným pacientem stále existuje z důvodu dodatečných informací zpracované zdravotnickým zařízením (v tomto případě IKEM).

- Pro úplnost uvádím, že údaje zpracované dodavatelem a IKEM při poskytování telemedicíny představují tzv. Speciální kategorie osobních údajů, které vyžadují zvýšenou ochranu.

Správce a Zpracovatel

- Během kontroly DPA dále posoudil postavení IKEM a příslušných dodavatelů při zpracování osobních údajů pacientů IKEM.

- Zákon o ochraně osobních údajů i GDPR rozpoznávají dvě základní pozice týkající se zpracování osobních údajů (a) správce a (b) zpracovatele.

- DPA dospěl k závěru, že IKEM (nebo zdravotní zařízení obecně) je vždy v postavení správce při poskytování telemedicíny.

- Pokud jde o dodavatele, DPA uznal, že dodavatel může buď jednat jako (a) zpracovatel pro IKEM, nebo (b) nezávislý správce.

- Vzhledem k výše uvedeným skutečnostem může být vztah mezi IKEM (zdravotnickým zařízením) a dodavatelem (poskytovatelem služeb telemedicíny) buď (a) správce zpracovatel, nebo (b) správce správce.

Vztah : Správce a Zpracovatel

- Ve vztahu správce ke zpracovateli se poskytovatel telemedicínské služby neřídí jako nezávislý subjekt, ale pouze jako dodavatel zdravotnického zařízení.
- Poskytovatel telemedicínských služeb zpracovává osobní údaje pouze pro účely stanovené zdravotnickým zařízením a podle jeho pokynů.

- Z pohledu zdravotnického zařízení je hlavní výhodou vztahu mezi správcem a zpracovatelem větší kontrola zpracovávaných dat.
- Na druhé straně je zdravotnické zařízení odpovědné za zpracování provedené poskytovatelem telemedicíny.
- Toto nastavení obecně vyžaduje písemnou dohodu o zpracování osobních údajů uzavřenou mezi zdravotnickým zařízením a poskytovatelem služeb telemedicíny (podrobnosti dále).

Výhody	Nevýhody
• **IKEM (zdravotní zařízení) řídí zpracovávané osobní údaje** • **IKEM (zdravotní zařízení) nemusí získat souhlas subjektu údajů k přenosu svých údajů na poskytovatele telemedicínských služeb**	• **IKEM (zdravotní zařízení) odpovídá za zpracování provedené poskytovatelem telemedicíny**

Vztah : Správce a Správce

- Ve vztahu správce vs správce fungují jak zdravotnické zařízení, tak poskytovatel telemedicínských služeb jako dva nezávislé subjekty.
- Toto nastavení vyžaduje, aby poskytovatel telemedicínských služeb získal zvláštní právní nárok na jeho zpracování, protože se nemůže spoléhat na právní nárok zdravotnického zařízení.

- Z pohledu zdravotnického zařízení je hlavní výhodou vztahu mezi správcem a správcem, že zdravotnická zařízení sama o sobě není zodpovědná za zpracování provedené poskytovatelem telemedicínských služeb.
- Na druhé straně, pokud není dohodnuto jinak, zdravotní zařízení nemá kontrolu nad tímto zpracováním.
- Tento scénář je obecně také náročnější na správu (vyžaduje získání souhlasu subjektů údajů s přenosem dat a jejich zpracováním poskytovatelem telemedicíny).

Výhody	Nevýhody
• IKEM (zdravotní zařízení) nenese odpovědnost za zpracování provedené dodavatelem (poskytovatelem služeb telemedicíny) • Není třeba uzavírat dohodu o zpracování dat mezi IKEM a dodavatelem	• IKEM potřebuje souhlas pacientů s přenosem osobních údajů dodavateli • Dodavatel potřebuje souhlas pacienta se zpracováním provedeným tímto dodavatelem • Zpracování založené na souhlasu je obecně rizikovější a méně spolehlivé • Není-li dohodnuto jinak, společnost IKEM nemá kontrolu nad zpracováním prováděnou dodavatelem • Obecně platí, že vztahy mezi správcem a správcem jsou mnohem vzácnější

Smlouva o zpracování osobních údajů

- Ve vztahu mezi správcem a zpracovatelem, pokud zákon nevyžaduje jinak, uzavře příslušný správce a zpracovatel písemnou dohodu o zpracování osobních údajů.
- Hlavním účelem této dohody je zajistit odpovídající ochranu zpracovávaných údajů.
- Podle GDPR tato dohoda mimo jiné zahrnuje následující opatření:

GDRP arrangement	Komentář/vysvětlení
Typ osobních údajů a kategorií subjektů údajů	Dohoda se týká kategorií osobních údajů zpracovaných poskytovatelem telemedicíny. Měla by také uvést, že se zpracovávají zvláštní kategorie osobních údajů (např. Údaje týkající se zdraví). Dohoda také stanoví kategorie dotyčných subjektů údajů (např. Pacientů).
Instrukce od správce	Poskytovatel telemedicíny zpracovává osobní údaje pouze na základě zdokumentovaných pokynů zdravotnického zařízení.
Důvěrnost	Poskytovatel telemedicíny zajistí, aby osoby zpracovávající osobní údaje byly vázány povinností zachovávat důvěrnost.
Bezpečnost osobních údajů	Poskytovatel telemedicíny provádí příslušná technická a organizační opatření k zajištění úrovně bezpečnosti odpovídající rizikům spojeným se zpracováním. Doporučuje se, aby do dohody byly zahrnuty minimální bezpečnostní normy.
Další zpracovatelé	Dohoda by měla stanovit pravidla pro zapojení takzvaného dalšího zpracovatele k provádění konkrétních zpracovatelských činností pro poskytovatele telemedicíny.
Spolupráce	Poskytovatel telemedicíny spolupracuje se zdravotnickým zařízením (např. Při poskytování součinnosti zdravotnímu zařízení s žádostmi subjektů údajů v rámci GDPR, v případě bezpečnostího incidentu či uníku údajů nebo při posuzování dopadů ochrany údajů). Poskytovatel telemedicíny rovněž povolí audity a inspekce prováděné zdravotnickým zařízením.
Ukončení zpracování	Dohoda obsahuje pravidla týkající se ukončení zpracování. Zdravotní zařízení rozhodne, zda poskytovatel telemedicíny vrátí nebo odstraní data.

Zabezpečení osobních údajů

- Poskytování péče v oblasti telemedicíny na kardiologické klinice IKEM bylo nedávno předmětem kontroly prováděné DPA.
- DPA zhodnotil (mimo jiné) bezpečnost osobních údajů zpracovávaných IKEM.
- DPA nenalezl v této oblasti žádné nedostatky a ve své závěrečné zprávě prohlásil přiměřenost organizačních a technických bezpečnostních opatření zavedených IKEM.

- Bezpečnostní opatření, která DPA pozitivně hodnotila v současné inspekci a její minulé praxi, jsou uvedeny zde :

Bezpečnostní opatření	Komentář/vysvětlení
Pseudonymizace	Zpracování osobních údajů takovým způsobem, že zpracovávaná data nelze přiřadit konkrétnímu subjektu údajů (fyzické osobě) bez použití dalších informací. Takové dodatečné informace jsou uchovávány odděleně a podléhají technickým a organizačním opatřením. V kardiologickém oddělení IKEM dodavatelé obecně neposkytují údaje, které by jim umožňovaly přímo identifikovat příslušného pacienta (např. Jméno, datum narození atd.), Ale zpracovávají pouze číslo pacienta a související údaje. S ohledem na výše uvedené skutečnosti v případě porušení osobních údajů (např. Neoprávněný přístup k osobním údajům) není přístupná osoba schopna určit totožnost dotčených fyzických osob. Proto je nepravděpodobné, že by porušování osobních údajů mělo za následek vysoké riziko pro práva a svobody subjektů údajů.
Šifrování	Proces šifrování dělá osobní údaje nečitelnými, dokud nebudou dešifrovány speciálním dešifrovacím klíčem. Použití šifrování omezuje přístup k osobním údajům oprávněným osobám s dešifrovacím klíčem. Veškerá komunikace mezi kardiologickým oddělením IKEM a příslušným dodavatelem je šifrována.
Přístupová práva	Přístup k zpracovávaným osobním údajům je poskytován pouze konkrétním zaměstnancům a zdravotnickým pracovníkům a v rozsahu nezbytném k poskytování zdravotní péče a telemedicínských služeb. Osoby, které přistupují k osobním údajům, jsou vázány příslušnými zásadami ochrany osobních údajů.
Logy	Správce i zpracovatel uchovávají záznamy o zpracovatelských činnostech, které jim umožňují prokázat soulad s GDPR. Logy monitorují a) kdo a kdy přistupuje k osobním údajům a b) zpracování, které tato osoba provádí.

Děkuji za pozornost

IK+E
M