HOLUBOVÁ.CZ

+420 224 914 050
info@holubova.cz
www.holubova.cz

Holubová advokáti s. r. o.
Za Poříčskou bránou 21/365, CZ 186 00 Praha 8
ID datové schránky: eaqq73c

Centrum paliativní péče, z.ú.
Dykova 1165/15
101 00 Praha 10 – Vinohrady

Analýza k informování pacienta o zdravotním stavu online

I. Zadání

Centrum paliativní péče, z.ú. (dále jen „centrum“) požádalo advokátní kancelář Holubová advokáti s.r.o. o vypracování analýzy k některým aspektům týkajícím se komunikace mezi pacienty a lékaři na dálku, typicky online. Tato problematika nabyla na významu zejména v souvislosti s epidemií nemoci Covid-19, která znesnadnila osobní komunikaci mezi lékařem a pacientem.

Cílem této analýzy je zjistit, za jakých podmínek mohou lékaři a pacienti komunikovat na dálku a jaká zařízení/aplikace jsou vhodné pro tuto komunikaci.

II. Relevantní právní rámec

- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen „zákon o kybernetické bezpečnosti“);
- Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (dále jen „zákon o elektronických komunikacích“);
- Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (dále jen „GDPR“);
- Zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách) (dále jen „ZZS“)

III. Ostatní zdroje

- Metodický pokyn Ministerstva zdravotnictví ČR a Ústavu zdravotnických informací a statistiky ČR: Jak implementovat v ambulantní sféře Nařízení Evropského parlamentu a Rady 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES v rezortu zdravotnictví, dostupné z: https://www.mzcr.cz/wp-content/uploads/wepub/15782/34328/gdpr_AMBUL_20180509__metodika_implementace_ambulantni_sfera.pdf

- Bezpečnostní standard pro videokonference vydaný Národním úřadem pro kybernetickou a informační společnost a Národní agenturou pro komunikační a informační technologie, dostupné z: https://nukib.cz/download/publikace/podpurne_materialy/2020-07-17_Standard-pro-VTC_1.0.pdf
- Úřad pro ochranu osobních údajů, poradna ze školství, sekce často kladených otázek, dostupné z: https://www.uoou.cz/ze%2Dskolstvi/ds-5088/p1=5088

IV. Analýza

A. Možnost komunikace na dálku s pacienty podle ZZS

ZZS v § 31 upravuje povinnost poskytovatele zdravotních služeb zajistit, aby byl pacient srozumitelným způsobem a v dostatečném rozsahu informován o svém zdravotním stavu a o navrženém léčebném postupu a všech jeho změnách. Dále § 31 ZZS upravuje povinnost poskytovatele zdravotních služeb umožnit pacientovi klást doplňující otázky vztahující se k jeho zdravotnímu stavu a o navrhovanému léčebnému postupu. Tyto dotazy je poskytovatel zdravotních služeb povinen zodpovědět.

ZZS určuje obsah poskytovaných informací a osobu, která je oprávněna tyto informace poskytnout. ZZS ale nestanovuje způsob komunikace s pacienty. Jelikož účelem příslušných ustanovení ZZS je srozumitelně a efektivně realizovat práva pacienta, může poskytovatel zdravotních služeb komunikovat s pacienty jakýmkoliv vhodným způsobem, ať už se jedná o komunikaci osobní, e-mailovou, telefonickou nebo prostřednictvím online videohovorů.

Nicméně, je třeba si uvědomit, že samotný přenos informace a zařízení/aplikace, která přenos zajišťují, představují určitá rizika. Za prvé se jedná o riziko toho, aby byla informace předána právě a jen pacientovi (riziko 1 – ověření totožnosti pacienta). Za druhé se jedná o riziko, že informace mohou být osobou, která zajišťuje přenos těchto komunikací, dále zpracovány nad rámec ZZS, například mohou být využívány k marketingovým účelům (riziko 2 – využití informací k jiným účelům). A za třetí jsou hrozbou různé kybernetické útoky, neoprávněný přístup jiných osob a s tím spojené zneužití osobních údajů (riziko 3 – bezpečnost). Na tyto tři okruhy se v této analýze dále zaměřujeme.

B. Analýza jednotlivých rizik

a. Riziko 1 – ověření totožnosti pacienta nebo jiné oprávněné osoby

Je povinností poskytovatele zdravotních služeb zajistit, že informace adresovaná pacientovi bude sdělena právě tomu pacientovi.

Při osobní komunikaci lékaře a pacienta je totožnost ověřována zpravidla na základě občanského průkazu a/nebo kartičky zdravotní pojišťovny. Dále je často při první návštěvě smluveno heslo, na základě kterého bude lékař poskytovat informace telefonicky buď samotnému pacientovi, nebo osobě, kterou pacient uvede. Toto je dostatečný a přiměřený způsob ověření totožnosti.

V případě komunikace prostřednictvím videokonference lze postupovat jako v případě osobní komunikace. Pacient je buď již lékaři znám a pamatuje si ho, nebo se již stávající pacient prokáže „na kameru“ občanským průkazem nebo průkazem pojištěnce.

b. Riziko 2 – využití informací k jiným účelům

Druhé myslitelné riziko se váže specificky na komunikaci prostřednictvím nových technologií, a to aplikací typu Zoom, Skype, WhatsApp a jiné. Tyto aplikace zpravidla využívají uložené údaje uživatelů a dále je zpracovávají. Právní předpisem, který danou problematiku upravuje, je Obecné nařízení o ochraně osobních údajů, tzv. GDPR.

GDPR definuje jako osobní údaje veškeré informace o identifikované nebo identifikovatelné fyzické osobě. Vůči poskytovateli zdravotních služeb je pacienta nutné považovat za identifikovanou osobu a veškeré informace, které o něm poskytovatel zdravotních služeb má, je nutné považovat za osobní údaje. Vzhledem k poskytovateli aplikace může být pacient identifikovatelná osoba. Aplikace nemusí znát přesné jméno, příjmení či rodné číslo, ale bude v každém případě znát e-mail, IP adresu a chování pacienta v rámci aplikace. Veškeré informace, které o pacientovi poskytovatel aplikace má, je nutné považovat za osobní údaje.

GDPR definuje skupinu osobních údajů jako zvláštní kategorii osobních údajů, resp. citlivých osobních údajů. Jedná se o osobní údaje, kterým GDPR přiznává vyšší ochranu. Mezi tyto údaje se řadí též údaje o zdravotním stavu. Údaji o zdravotním stavu jsou též osobní údaje týkající se tělesného nebo duševního zdraví fyzické osoby, včetně údajů o poskytnutí zdravotních služeb, které vypovídají o jejím zdravotním stavu. Je zjevné, že v případě komunikace mezi lékařem a pacientem prostřednictvím aplikací jsou zpracovávány citlivé osobní údaje.

Zpracováním osobních údajů se podle GDPR rozumí jakákoliv operace nebo soubor operací s osobními údaji, která může, ale nemusí být prováděna automatizovaně. Jako příklad zpracování osobních údajů GDPR uvádí shromáždění, zaznamenání, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění osobních údajů. Zpracováním osobních údajů je tedy i zpřístupnění přenosem, tedy sdělení pacientovi online či uložení v samotné aplikaci.

Dílčí závěr: Poskytovatel zdravotních služeb zpracovává citlivé osobní údaje o pacientovi v tom smyslu, že je pacientovi prostřednictvím online aplikace sděluje, zaznamenává nebo vpisuje do chatu.

Pro určení povinností poskytovatele vůči pacientovi z hlediska GDPR je třeba odlišit pozice správce osobních údajů, zpracovatele osobních údajů a subjektu údajů.

Správce osobních údajů je definován jako fyzická nebo právnická osoba, která sama nebo společně s jinými určuje účely a prostředky zpracování osobních údajů. Dále je v GDPR uvedeno, že v případě, že je účel a prostředky zpracování určen právem členského státu EU, pak toto právo může určit dotčeného správce nebo zvláštní kritéria pro jeho určení. Poskytování zdravotní péče je upraveno v ZZS. Na základě ZZS je nutné dovodit, že poskytovatel zdravotních služeb je správcem osobních údajů. Odpovídá tedy za to, komu budou osobní údaje pacienta předány.

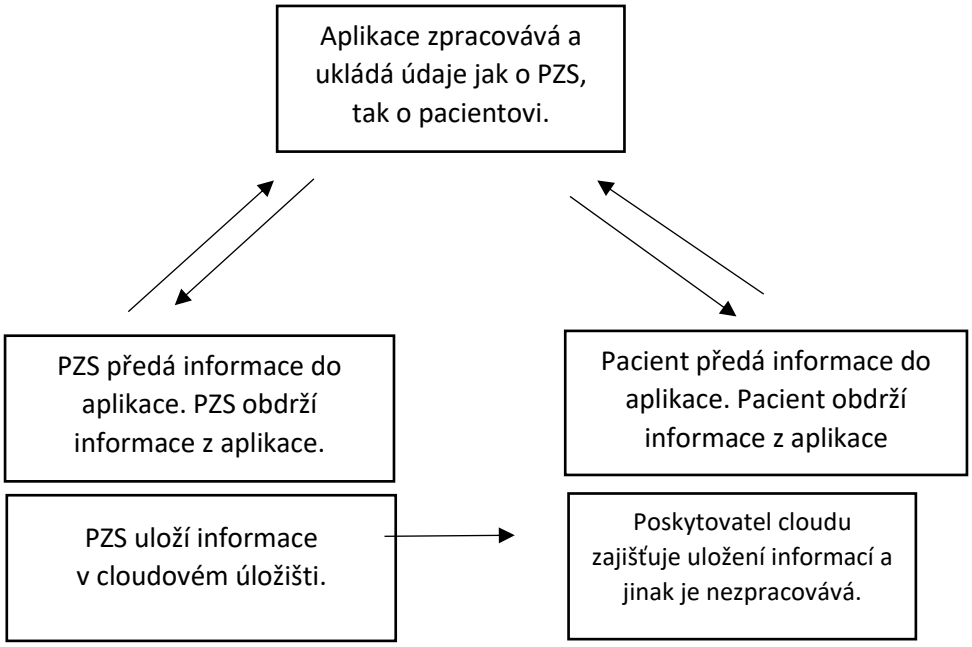
Subjekt osobních údajů je fyzická osoba, které se osobní údaje týkají. Pacient je subjektem údajů.

Zpracovatelem osobních údajů je fyzická nebo právnická osoba, která zpracovává osobní údaje pro správce osobních údajů. Význam rozlišování na správce a zpracovatele spočívá v tom, že mezi správcem a zpracovatelem musí být uzavřena smlouva o zpracování osobních údajů (zpracovatelská smlouva). Správce vůči subjektu údajů odpovídá za činnost

zpracovatele. Typickým zpracovatelem je poskytovatel úložiště nebo poskytovatel e-mailu. V odborných publikacích není doposud jasně stanoveno, zda i aplikace typu Zoom jsou zpracovatelé nebo samostatní správci osobních údajů. Dle našeho názoru se jedná o samostatné správce osobních údajů. Mezi dvěma správci zpracovatelská smlouva uzavřena být nemusí a každý správce odpovídá sám za zpracování osobních údajů.

GDPR dále vymezuje pojem příjemce osobních údajů. Příjemcem osobních údajů je fyzická nebo právnická osoba, které jsou osobní údaje poskytnuty.

Popsanou situaci zpracování osobních údajů při využívání aplikací můžeme znázornit takto:



Dílčí závěr: Jelikož poskytovatel zdravotních služeb i poskytovatel aplikace jsou samostatnými správci osobních údajů, neuplatní se mezi nimi pravidla pro správce a zpracovatele, zejména nejsou povinni uzavřít zpracovatelskou smlouvu.

Nicméně i tak má poskytovatel zdravotních služeb některé povinnosti. Je třeba si uvědomit, že je to právě poskytovatel zdravotních služeb, který osobní údaje poskytovateli aplikace předává, z jeho sféry se dostávají do sféry soukromého subjektu. Tyto informace ukládá poskytovatel aplikace na cloudovém úložišti samotné aplikace.

Zpracování osobních údajů, a tedy i předání osobních údajů poskytovateli aplikace, se musí vždy zakládat na právním důvodu vyjmenovaném v čl. 6 nebo čl. 9 GDPR. Čl. 6 upravuje právní důvody zpracování „běžných“ osobních údajů. Čl. 9 zakazuje zpracovávat citlivé osobní údaje až na vyjmenované výjimky. Pro případ komunikace s pacientem jsou relevantní:

- pacient udělil výslovný souhlas;[1]
- zpracování je nezbytné pro účely poskytování zdravotní nebo sociální péče či léčby;[2]
- zpracování je nezbytné z důvodů veřejného zájmu v oblasti veřejného zdraví, jako je ochrana před vážnými přeshraničními zdravotními hrozbami;[3]

[1] Čl. 9 odst. 2 písm. a) GDPR.
[2] Čl. 9 odst. 2 písm. h) GDPR.
[3] Čl. 9 odst. 2 písm. j) GDPR.

Dle našeho názoru je sporné, zda se může použít důvod nezbytnosti pro účely poskytování zdravotní péče a nezbytnosti z důvodu ochrany veřejného zdraví. Poskytovatel má totiž možnost komunikovat s pacientem například telefonicky, kde je riziko dalšího užití údajů eliminováno zákonem. Proto je dle našeho názoru jediným možným právním důvodem předání osobních údajů poskytovateli aplikace výslovný souhlas pacienta. Tento souhlas musí splňovat obecné náležitosti souhlasu dle GDPR a dále by měl obsahovat podrobnější poučení rizik.

Pro ilustraci rizik uvádíme příklad toho, jak jsou osobní údaje zpracovány v placené aplikaci Zoom (Paid Zoom Account) a v aplikaci Zoom zdarma (Free Zoom Account). Na rozdíl od placeného účtu na účtu zdarma jsou zpracovány osobní údaje uživatele též pro pořádání soutěží loterií nebo jiných propagačních aktivit („run opt-in contests, sweepstakes or other promotional activities“).[4] Ve chvíli, kdy jsou tímto prostřednictvím jako oficiálním kanálem sdělovány informace o zdravotním stavu, může jejich následná komercializace ze strany poskytovatele aplikace zoom představovat závažné riziko pro pacienty.

V současnosti neexistuje stanovisko Úřadu pro ochranu osobních údajů, které by využívání těchto aplikací zakázalo nebo povolilo. Nicméně Úřad pro ochranu osobních údajů se již k této problematice vyjádřil v oblasti školství. K dotazu, za jakých podmínek může škola ke zpracování části osobních údajů využívat služeb externích dodavatelů, příp. služeb dostupných na internetu zdarma, uvedl:

„Z důvodu bezpečnosti, častých rizik v oblasti informačních systémů a hrozeb zneužití, krádeže i úniku údajů, je nutno důrazně doporučit v každém jednotlivém případě pečlivě zvažovat potřebnost uchovávání jakýchkoliv osobních údajů z agendy školy mimo informační systém školy, např. u dodavatelů systémů. Blíže viz výše uvedená metodika MŠMT.“[5]

Školy oproti poskytovatelům zdravotních služeb nezpracovávají až na výjimky citlivé osobní údaje, nároky na ochranu a zabezpečení jsou tak nižší než u poskytovatelů zdravotních služeb, kteří zpracovávají údaje o zdravotním stavu. Z toho důvodu nelze ani poskytovatelům zdravotních služeb doporučit, aby pro účely komunikace s pacienty využívali aplikace zdarma.

Aplikace určené pro odborné použití však zpravidla nebudou zpracovávat osobní údaje nad rámec zakoupené licence, zejména pro některé marketingové účely. Marketingově je bude zpracovávat v souladu s nastavením webového prohlížeče.

Dílčí závěr: Poskytovatelům zdravotních služeb lze doporučit, aby nepoužívali aplikace zdarma, ale naopak využívali profesionální verze těchto aplikací. Vždy však budou potřebovat pro účely předání citlivých osobních údajů poskytovateli aplikace výslovný souhlas pacienta s náležitostmi dle GDPR.

c. Riziko 3 – Bezpečnost

Třetí myslitelné riziko se váže na samotné zabezpečení komunikace a její důvěrnosti, a dále možnost zneužití informací. Tuto problematiku upravuje jednak GDPR a jednak zákon o kybernetické bezpečnosti.

Co se týče zákona o kybernetické bezpečnosti, ten v § 2 písm. i) bod. 5 definuje základní službu jako služba, jejíž poskytování je závislé na sítích elektronických komunikací nebo informačních systémech a jejíž narušení by mohlo mít významný dopad na zabezpečení společenských nebo ekonomických činností v odvětví zdravotnictví. Ačkoliv by se tedy na první pohled mohlo zdát, že zákon o kybernetické bezpečnosti se na komunikaci mezi lékařem

[4] Dostupné z: https://zoom.us/privacy#_Toc44414842

[5] Dostupné zde: https://www.uoou.cz/ze%2Dskolstvi/ds-5088/p1=5088

a pacientem prostřednictvím online aplikací mohl vztahovat, není tomu tak. Narušení/napadení této komunikace by totiž nemělo významný dopad v oblasti zdravotnictví. Toto ustanovení míří například na informační systémy používané v rámci celé nemocnice, příp. registry spravované ministerstvem, např. lékový záznam. Zákon o kybernetické bezpečnosti se tak na komunikaci mezi pacientem a lékařem prostřednictvím online aplikací, pokud se nejedná o systémové řešení, nevztahuje.

S ohledem na GDPR je třeba říci, že každý správce je povinen vhodně zabezpečit osobní údaje. Jelikož samotný poskytovatel aplikace je správcem osobních údajů, není odpovědností poskytovatele zdravotních služeb to, jak budou informace uložené v aplikaci využity, příp. zda budou zneužity. Nicméně poskytovatel zdravotních služeb odpovídá za vhodné zabezpečení údajů, kterých je správcem.

GDPR nestanoví, co se považuje za vhodné zabezpečení osobních údajů. To je třeba posuzovat vždy jednotlivě a s ohledem na rozsah zpracovávaných údajů a jejich citlivost. Vhodným vodítkem může být dokument nazvaný Bezpečnostní standard pro videokonference vydaný Národním úřadem pro kybernetickou a informační společnost a Národní agenturou pro komunikační a informační technologie.[6] Ačkoliv se jedná o dokument doporučující a nezávazný, je dle našeho názoru velmi zdařilý a reflektuje různou citlivost online komunikace.

Dílčí závěr: Poskytovatel zdravotních služeb má obecnou povinnost zajistit vhodné zabezpečení osobních údajů pacienta. Je na jeho uvážení, jakým způsobem tak učiní, přičemž, pokud jde o technickou specifikaci nastavení videohovorů, může využít dokument Bezpečnostní standard pro videokonference.

V. Závěr

Analyzovali jsme tři základní rizika, které se pojí s problematikou komunikace mezi lékařem a pacientem prostřednictvím online aplikací. Jedná se o riziko sdělení informací osobě odlišné od pacienta, riziko dalšího využití osobních údajů samotným poskytovatelem aplikace a bezpečnostní rizika spojená s virtuálním prostředím. Došli jsme k závěru, že všechna tato rizika se dají prostřednictvím vhodných postupů eliminovat a tím nastavit situaci, kdy je online komunikace mezi pacienty a lékaři legální.

V rámci analýzy jsme upozornili, že poskytovatel zdravotních služeb zpracovává citlivé osobní údaje o pacientovi v tom smyslu, že je pacientovi prostřednictvím online aplikace sděluje, zaznamenává nebo vpisuje do chatu.

Dále jsme upozornili, že poskytovatel zdravotních služeb i poskytovatel aplikace jsou samostatnými správci osobních údajů, a proto se mezi nimi neuplatní pravidla určená pro vztah mezi správcem a zpracovatelem, zejména nejsou povinni uzavřít zpracovatelskou smlouvu.

Z analýzy vyplývá, že poskytovatelům zdravotních služeb nelze doporučit, aby pro účely online hovorů používali aplikace zdarma, ale naopak využívali profesionální verze těchto aplikací. Nicméně, i pokud používají profesionální licence, budou vždy potřebovat pro účely předání citlivých osobních údajů poskytovateli aplikace výslovný souhlas pacienta s náležitostmi dle GDPR.

[6] Dostupný zde: https://nukib.cz/download/publikace/podpurne_materialy/2020-07-17_Standard-pro-VTC_1.0.pdf

Konečně, poskytovatel zdravotních služeb má nejen povinnost zajistit souhlas pacienta, pokud hodlá sdělovat jeho osobní údaje prostřednictvím aplikace, ale má také obecnou povinnost zajistit vhodné zabezpečení osobních údajů pacienta. Je na jeho uvážení, jakým způsobem tak učiní, přičemž, pokud jde o technickou specifikaci nastavení videohovorů, může využít doporučení uvedená v dokumentu Bezpečnostní standard pro videokonference.

Praha 4. 11. 2020

Holubová advokáti s.r.o.