Směrnice určuje práva a povinnosti pracovníků správce osobních údajů ve vztahu k ochraně osobních údajů. Upravuje též konkrétní režim na pracovišti, způsoby zabezpečení (fyzického i elektronického).

Směrnice upravující eliminaci rizik při správě osobních údajů – technicko-organizační opatření

Obsah

- **Účel**

Tento pracovní postup stanovuje pravidla pro řízení rizik při zpracování osobních údajů u poskytovatele zdravotních služeb jako Správce. Správce zpracovává osobní údaje při:

- vedení zdravotnické dokumentace ve zdravotnickém zařízení;
- vedení objednávacích systémů
- vedení adresářů pacientů
- zpracování výkazů pro zdravotní pojišťovny
- účetních a daňových operacích
- vedení evidence stížností
- vedení přístrojových deníků a záznamů ke zdravotnickým prostředkům
- vedení seznamů vyřazené dokumentace
- vedení osobních spisů zaměstnanců
- vedení evidence a hlášení nežádoucích příhod a nežádoucích účinků
- vedení evidence daňových dokladů vystavených dodavateli.

- **Oblast platnosti**

Tento pracovní postup je závazný pro všechny zaměstnance poskytovatele.

- **Pojmy a zkratky**
- **Pojmy**

Riziko

- je obecně pravděpodobnost výskytu nežádoucí události s negativními dopady
- je spojeno s pravděpodobností nebo možností vzniku škody
- je kvantitativní a kvalitativní vyjádření ohrožení

- vyjadřuje pravděpodobnost, že nastane negativní jev
- vyjadřuje, kolikrát se negativní jev vyskytne a co způsobí
- definuje se jako kombinace pravděpodobnosti nežádoucí události a rozsahu, závažnosti možného zranění, škody nebo poškození zdraví.

Míra rizika – kombinace pravděpodobnost vzniku události a následků, které tato událost může způsobit.

Analýza rizik – základní a nezbytný krok pro zvládání řízení rizik v organizaci, zvláště pak těch rizik, která ohrožují správný chod organizace.

• Prevence a řízení rizik

Prevencí rizik se rozumí všechna opatření, která mají za cíl předcházet rizikům, snižovat je na přijatelnou úroveň a realizovat účinná preventivní opatření k jejich odstranění.

Podmínkou účinné a účelné prevence rizik je jejich identifikace a porozumění jejich příčinám. Proto je organizace povinna rizika vyhledávat, zjišťovat jejich příčiny a zdroje a přijímat příslušná opatření.

Pro hodnocení rizik a zjištění jejich příčin a zdrojů se používají různé metody, které se od sebe liší mírou objektivity, pracností a účelem, ke kterému má hodnocení rizik sloužit. Zvolení metody je na zvážení organizace.

• Analýza rizik

Největší překážkou při hodnocení rizik je obvykle nedostatek dat a informací. Protože hodnocení rizik slouží jako základní zdroj informací pro rozhodování, je důležité znát a být si vědom omezení použitých metod. Základní podmínkou je dostatečná transparentnost jednotlivých kroků, jak pro uživatele výsledků hodnocení, tak pro ty, jichž se následky rizika mohou dotknout.

• Pracovní postup

- Poskytovatel je odpovědný za zpracování „Katalogu rizik“.
- Aktualizace Katalogu rizik probíhá podle potřeb.

• Základní zásady eliminace rizik

- Ochrana osobních údajů je zajišťována prostřednictvím ochrany médií/zařízení, která se používají k jejich zaznamenání. Tato ochrana je nezbytná pro snížení rizika neautorizovaného přístupu k datům a k zajištění ochrany proti ztrátě nebo poškození. Pozornost musí být věnována umístění a likvidaci médií/zařízení, která osobní údaje obsahují.
- Média/Zařízení musí být umístěna a chráněna tak, aby se snížila rizika hrozeb a nebezpečí daná prostředím a aby se omezily příležitosti pro neoprávněný přístup.
- V případě použití elektronických zařízení pro zpracování a uchování osobních dat musí být zařízení chráněno před selháním napájení (např. použití záložních zdrojů UPS) a před dalšími výpadky způsobenými selháním podpůrných služeb.
- Ochrana proti škodlivým programům je založena na detekci škodlivých programů, opravných programů a na bezpečnostním povědomí uživatelů. Instalace a pravidelná aktualizace antivirových detekčních a opravných programů pro kontrolu počítačů a médií je prováděna pravidelně a ve výjimečných případech ad-hoc způsobem.
- Záložní kopie důležitých informací a programového vybavení organizace jsou pořizovány a testovány v pravidelných intervalech. Záložní kopie zdravotnické dokumentace je pořizována v intervalech stanovených právními předpisy.

- Zálohy jsou ukládány na bezpečném místě, v dostatečné vzdálenosti od ordinace, aby v případě havárie nebyly poškozeny nebo zničeny.
- Při správě vyměnitelných médií obsahujících osobní údaje je nutno dbát potřebné opatrnosti. Pokud média obsahují osobní údaje a jsou dále provozně neupotřebitelná, měla by být bezpečně zlikvidována, například spálením, skartováním nebo smazáním dat před jejich opětovným použitím jiným způsobem v rámci Správce.
- Pro zabránění neautorizovanému přístupu nebo zneužití osobních údajů jsou stanovena zvláštní pravidla pro manipulaci s nimi a pro jejich ukládání (viz Přílohy č. 2-5).
- Přístupová pravidla a oprávnění k osobním údajům jsou jasně stanovena pro každého uživatele (viz Přílohy č. 3, 4) a jsou pravidelně monitorována a kontrolována.
- Všichni zaměstnanci užívají jako způsob autentizace při použití výpočetní techniky k ověření své identity heslo.
- Při použití mobilní výpočetní techniky jsou přijata zvláštní opatření na ochranu proti rizikům použití mobilních výpočetních a komunikačních prostředků (viz Příloha č. 5)
- Média/zařízení, na nichž jsou osobní údaje uloženy, jsou skladována a archivována pouze po nezbytně nutnou dobu (zásada minimalizace).

- **Přílohy**

Příloha č. 1: Katalog rizik
Příloha č. 2: Plán eliminace rizik při vedení dokumentace v elektronické podobě
Příloha č. 3: Plán eliminace rizik při vedení zdravotnické dokumentace v listinné podobě
Příloha č. 4: Plán eliminace rizik při správě osobních údajů mimo režim zdravotnické dokumentace
Příloha č. 5: Plán eliminace rizik při použití mobilní výpočetní techniky

Příloha č. 1: Katalog rizik

Katalog rizik

Druh hrozby	Možné příčiny vzniku
Narušení důvěrnosti údajů *(s údaji seznámil někdo, kdo k tomu neměl oprávnění)*	• nedostatečné zabezpečení sítě • prolomení přístupových práv uživatelů • neexistence IT bezpečnostní strategie • nezabezpečení dat při výpadku informačních systémů • nedostatečné zabezpečení přenosu dat • nedostatečná antivirová ochrana • nedostatečné nastavení bezpečnosti IT infrastruktury • možnost nahrávat data pacientů na nosiče (CD, DVD, flash disk, externí hard disk) • nedodržování pravidel při předávání důvěrných informací o zdrav. stavu • chybějící záznam souhlasu s poskytováním informací o zdrav. stavu • chybná volba vhodného místa pro předávání informací • porušení povinnosti zachovávání mlčenlivosti • nedostatečné ověření totožnosti osob určených pacientem k poskytování informací • únik dat ze systému

	• nezabezpečený přístup do papírové i elektronické dokumentace (volně přístupné kartotéky, klíče ve dveřích z vnější strany, neodhlášení se z PC atd.)
Narušení integrity údajů *(údaje byly pozměněny či upraveny)*	• provozování kritických prvků výpočetní techniky nad mez životnosti • používání kritických prvků bez zabezpečení podpory • nedostatečné zabezpečení sítě • prolomení přístupových práv uživatelů • neexistence IT bezpečnostní strategie
Narušení dostupnosti údajů *(údaje sice existují, nelze je ale použít)*	• fyzická ztráta zdravotnické dokumentace • nedostatečné znalosti a kvalifikace personálu, selhání lidského činitele, nedostatečné proškolení uživatelů IS nebo správců, administrátorů IS • porušení interních předpisů • nekonzistence dat v důsledku chyb IS • provozování kritických prvků výpočetní techniky nad mez životnosti
Ztráta údajů *(údaje byly nenávratně ztraceny)*	• nezabezpečení při výpadku informačních systémů (serverů) • nedostatečná antivirová ochrana • nedostatečná kontrola • nedostatečné nastavení bezpečnosti IT infrastruktury • chybné nastavení IS • nedostatečné znalosti a kvalifikace personálu, uživatelů IS • počítače, výpočetní a archivační technika používaná nad mez životnosti • nedostatečná kontrola • nebezpečí krádeže, nedostatečný režim uložení přístupových klíčů • nedostatečná kontrola vhodnosti prostředí pro IT (provozní teplota, vlhkost atd.) • nebezpečí vzniku požáru • zastarání techniky, datových médií

Příloha č. 2:

Plán eliminace rizik při vedení dokumentace v elektronické podobě

Povinnosti jednotlivých zaměstnanců, které souvisejí s bezpečností a nakládání s daty a elektronickými dokumenty:

- při zpracovávání informací pomocí výpočetní techniky musí být především zabezpečena ochrana všech dat uložených na pevném disku počítače, přičemž se zde uplatňuje vždy ochrana heslem a stanovením rozsahu jednotlivých přístupových oprávnění v souladu s pracovní náplní toho konkrétního zaměstnance. Dále platí pravidlo, že pokud má uživatel oprávnění vkládat či měnit data uložená v systému, musí být zajištěna jeho jednoznačná identifikace při jeho přístupu k datům,
- rozsah přístupu k datům a informacím a oprávnění k jejich využívání, včetně změn, vkládání nebo případného vymazání dat, musí odpovídat obsahu pracovních povinností, které má zaměstnanec podle jeho pracovního zařazení a právním předpisům

- za určení rozsahu přístupových práv každému zaměstnanci jako uživateli IT techniky a informačního systému odpovídá poskytovatel
- za samotné nastavení rozsahu přidělených přístupových práv každému zaměstnanci odpovídá správce IT
- pro zálohování dat a archivaci vedených pomocí výpočetní techniky platí zvláštní předpis, přičemž ta data, která se nearchivují, musí být neustále a bezpečně zálohována do té doby, než dojde podle příslušného právního předpisu nebo dohody smluvních stran k jejich skartaci/zničení.
- pro zasílání údajů ze zdravotnické dokumentace a pro zasílání ereceptů a pro zasílání fotek plodu těhotným pacientkám je požíván program Fetview. Program umožňuje i profesionální konzultaci zdravotního stavu. Bezpečnost přenosu a ukládání dat je zapezpečena 256-Bit VPN kódováním. Pacienti udělují správci souhlas s touto komunikací a s ukládáním dat na server Fetview na dobu 1 roku od podpisu souhlasu.
- pro zasílání ereceptů a údajů ze zdravotnické dokumentace a žádanek příjemci emailem je používána i nezabezpečená komunikace a to pouze po poučení o nebezpečnosti této komunikace a po podpisu souhlasu příjemce s touto komunikací, souhlas je udělován až do odvolání příjemcem.

Příloha č. 3:

Plán eliminace rizik při vedení zdravotnické dokumentace v listinné podobě

Povinnosti jednotlivých zaměstnanců, které souvisejí s bezpečností a nakládání s daty a listinnými dokumenty:

- rozsah přístupu k datům a informacím a oprávnění k jejich využívání, včetně změn, vkládání nebo případného vymazání dat, musí odpovídat obsahu pracovních povinností, které má zaměstnanec podle jeho pracovního zařazení a právních předpisů;
- dokumentace je uchovávána odděleně a je k ní zajištěn pouze zabezpečený přístup (kartotéka je uzamykatelná nebo je pod stálým dohledem zaměstnance poskytovatele);
- po vyjmutí karty pacienta z kartotéky je karta přístupná pouze lékaři a sestře, příp. další osobám podle příslušných ustanovení z. č. 372/2011 Sb.; karta je následně ihned uložena zpět do kartotéky;
- veškeré nakládání se zdravotnickou dokumentací probíhá podle příslušných ustanovení z. č. 372/2011 Sb. a dalších právních předpisů.

Příloha č. 4:

Plán eliminace rizik při správě osobních údajů mimo režim zdravotnické dokumentace

Povinnosti jednotlivých zaměstnanců, které souvisejí s bezpečností a nakládání s daty v elektronické podobě a listinnými dokumenty mimo režim zdravotnické dokumentace:

- rozsah přístupu k datům a informacím a oprávnění k jejich využívání, včetně změn, vkládání nebo případného vymazání dat, musí odpovídat obsahu pracovních povinností, které má zaměstnanec podle jeho pracovního zařazení a právních předpisů;
- média/data jsou uchována na místech, kde je zabráněno vstupu neoprávněným osobám;
- osobní údaje jsou zpracovávány pouze v souladu se stanoveným účelem zpracování;

- přístupová pravidla a oprávnění k osobním údajům jsou pravidelně monitorována a kontrolována;
- média/zařízení, na nichž jsou osobní údaje uloženy, jsou skladována a archivována pouze po nezbytně nutnou dobu (zásada minimalizace). Po uplynutí této doby jsou skartována.

Příloha č. 5:

Plán eliminace rizik při použití mobilní výpočetní techniky

- Při použití mobilních výpočetních prostředků, například notebooků a mobilních telefonů musí být věnována zvláštní pozornost tomu, aby nebyly prozrazeny zpracovávané osobní údaje.
- Mobilní výpočetní prostředky musí být chráněny proti zcizení a možnosti získání osobních údajů v nich obsažených (např. vzdálené vypnutí, možnost vzdáleného vymazání dat). Zařízení, obsahující zpracovávané osobní údaje nesmí zůstávat bez dohledu, mělo by být fyzicky zabezpečeno nebo by jeho funkce měly být zajištěny speciálním uzamčením.
- Při použití mobilních výpočetních zařízení připojených k sítím musí být zajištěna vhodná ochrana (antivirový program, heslování) a vzdálený přístup k osobním údajům prostřednictvím veřejných sítí musí být umožněn pouze po úspěšné identifikaci a autentizaci, a to s nasazením vhodných mechanizmů řízení přístupu.
- Zvláštní pozornost musí být věnována použití mobilních výpočetních zařízení na veřejných místech a jiných nechráněných místech mimo prostor ordinace.