Ochrana osobních údajů

Zpracovatel:
Ing. Michal Jelínek
Roman Skuhra
Mgr. Zuzana Kandová

Garant:
Úsek informatiky

Účinnost dokumentu od:
2. 8. 2018

První vydání dne:
20. 3. 2008

Schválil:
Mgr. Dana Jurásková, Ph.D., MBA

Dne:
1. 8. 2018

Obsah:

Označení změn oproti minulé verzi.

1. Účel a oblast platnosti dokumentu

Tento dokument popisuje zásady pro ochranu osobních údajů zaměstnanců, pacientů a dalších osob na pracovištích a v prostorách VFN v souladu s platnou legislativou[1][2].

Dokument je závazný pro všechny zaměstnance VFN.

2. Pojmy a zkratky

Citlivý údaj Osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu subjektu atp.

ICT Informační a komunikační technologie (Information and Communication Technologies); souhrn technických prostředků (hardware - HW) a programového vybavení (software - SW) použitých k propojení počítačů a ostatních síťových zařízení, jejich komunikaci a zpracování dat a telekomunikační zařízení (telefony, faxy) atp.

Incident Závada ICT, jakýkoliv stav ohrožující bezproblémový chod ICT nebo bezpečnost informací a informačních prostředků, nežádoucí událost apod.

Informace jsou jakékoliv údaje, které jsou sdělovány, ukládány a zpracovávány v písemné, digitální, obrazové nebo zvukové (mluvené) formě o reálném prostředí, jeho stavu a o procesech v něm probíhajících.

IS Informační systém/systémy

Kamerový systém Automaticky provozovaný stálý technický systém umožňující pořizovat a uchovávat zvukové, obrazové nebo jiné záznamy ze sledovaných míst.

Lokální stanice HW zařízení, které je schopno ukládat lokálně data – např. PC (počítač – pracovní stanice), notebook, tablet, mobilní telefon atd.

Osobní údaj (OÚ) Jakýkoliv údaj týkající se určeného nebo určitelného subjektu údajů - lze na základě jednoho či více osobních údajů zjistit jeho identitu.

Porušení zabezpečení osobních údajů Jedná se o porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů.

Registr OÚ Registr zpracování osobních údajů VFN, kde jsou zaznamenány IS a úložiště listin obsahující osobní údaje.

ServiceDesk Nástroj na zaznamenání, evidenci a sledování stavu incidentů nebo požadavků zaměstnanců VFN a pracovníků externích dodavatelských firem řešených Úsekem informatiky.

Správa ICT Činnost, která zajišťuje plynulý chod HW a SW prostředků.

[1] Zákon č. 101/2000 Sb., o ochraně osobních údajů;
[2] Nařízení Evropského parlamentu a Rady (EU) č. 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 (obecné nařízení o ochraně osobních údajů); neboli GDPR (General Data Protection Regulation).

Správce ICT Zaměstnanci odborného útvaru, kteří zodpovídají za provoz a rozvoj ICT, zejména správu datových sítí, aktivních prvků datových sítí včetně serverů, používaného HW, seznamu uživatelů a řízení přístupu uživatelů, používaných aplikací apod.

Subjekt údajů Fyzická osoba, k níž se osobní údaje vztahují.

ÚOOÚ Úřad pro ochranu osobních údajů, který je dozorovým úřadem, který v České republice dohlíží na ochranu soukromí a osobních údajů.

OÚ Osobní údaj

Zpracování osobních údajů Jakákoli operace, kterou správce nebo zpracovatel systematicky provádějí s osobními údaji, zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace.

3. Odpovědnosti a pravomoci

Každý vedoucí zaměstnanec je odpovědný za dodržování zásad pro práci s osobními údaji (dále také OÚ) **na jemu podřízeném pracovišti**.

Všichni vedoucí zaměstnanci jsou povinni provádět v organizaci práce na podřízeném pracovišti taková opatření, aby bylo **zabráněno v přístupu** k osobním a citlivým údajům zaměstnancům nebo jiným osobám, kteří k výkonu své práce tyto údaje bezprostředně nepotřebují nebo k nim nemají mít přístup, a současně bylo zabráněno jejich využití například k přístupu do informačního systému nebo k dalším informacím.

Každý zaměstnanec VFN je povinen dodržovat zásady pro zacházení s osobními údaji a dbát na to, aby nemohlo dojít ke zneužití nebo odcizení údajů nepovolanými osobami nebo k jejich ztrátě. Zároveň je povinen upozornit na případy, kdy nejsou zásady pro práci s osobními údaji dodržovány a podle svých možností sjednat, pokud možno okamžitou, nápravu.

Pro všechny zaměstnance, kteří přicházejí jakýmkoliv způsobem do styku s osobními údaji zaměstnanců nebo pacientů nebo dalších subjektů, platí povinnost **dodržovat mlčenlivost** nejenom vůči osobám zvenčí, ale i vůči zaměstnancům VFN zakotvenou v platné legislativě[3][4][5], a to i po skončení pracovního poměru.

Vedení zdravotnické dokumentace musí být prováděno striktně v souladu se zákonem č. 372/2011 Sb., o zdravotních službách. Pokud jsou údaje ze zdravotnické dokumentace pacienta využívány také pro jiné účely než pro vedení dokumentace o zdravotním stavu pacienta (např. výzkum), musí vždy splňovat požadavky zákona č. 101/2000 Sb., o ochraně osobních údajů a nařízení EU č. 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Z tohoto důvodu musí být každé zpracování obsahující osobní údaje prováděno způsobem stanoveným v této směrnici.

Každý vedoucí zaměstnanec zajistí **nahlášení vzniku nového** shromažďování či zpracovávání OÚ **nebo provedené změny zpracování OÚ (v elektronické nebo papírové podobě)** zadáním

[3] Zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování;
[4] Zákon č. 101/2000 Sb., o ochraně osobních údajů;
[5] Nařízení Evropského parlamentu a Rady (EU) č. 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 (obecné nařízení o ochraně osobních údajů); neboli GDPR (General Data Protection Regulation).

požadavku do ServiceDesku a spolu s přiloženým vyplněným formulářem (F-VFN-445 Nahlášení/změny/ukončení zpracování osobních údajů), kdy na jemu podřízeném pracovišti dochází ke zpracování osobních údajů, a to:

- nové zpracování s předstihem, aby bylo možné posoudit před zahájením zpracování,
- při změně nebo zrušení zpracování nejpozději do 10 dnů.

Způsob hlášení je definován v kapitole 4.2 Evidence, zpracování, uložení a zabezpečení OÚ.

V případě zrušení zpracování OÚ na podřízeném pracovišti je vedoucí zaměstnanec povinen tuto skutečnost předem ohlásit ÚI zadáním požadavku do ServiceDesku včetně uvedení způsobu likvidace nosičů osobních údajů při dodržení spisového řádu a skartačního plánu[6]. Likvidaci datových nosičů provádí ÚI. Žádost o likvidaci datových nosičů se zadává prostřednictvím požadavku do ServiceDesku.

ÚI vede registr informačních systémů nebo úložišť listin s OÚ a odpovídá za zapracování aktualizací na základě nahlášení/změn/ukončení zpracování OÚ zadané prostřednictvím ServiceDesku.

Správcem osobních údajů pořízených z kamerového systému je pověřen pracovník **Útvaru bezpečnosti a krizové připravenosti** (dále jen „pověřený pracovník“), který zajišťuje posouzení oprávněnosti kamerového systému.

Způsob posouzení oprávněnosti je definován v kapitole 4.8 Kamerové systémy. Technickým správcem kamerového systému je pověřený zaměstnanec Odboru správy ICT.

Každý útvar VFN je povinen v případě, že pro VFN bude zpracovávat osobní údaje externí subjekt (např. externí zpracovatel, dodavatel SW nebo HW, outsourcer apod.), zakotvit do smlouvy na základě odsouhlasení LPO přesné podmínky a rozsah těchto činností, náležitostí ochrany osobních údajů, sankce při nedodržení a povinnost zachovávat mlčenlivost i po skončení tohoto smluvního vztahu. Vzor smluvních závazků ve vztahu k ochraně osobních údajů je uveden v příloze (Příloha č. 1 - Smluvní náležitosti ochrany osobních údajů) této směrnice.

Detailní informace o zpracování OÚ jsou dostupné na intranetu nebo webu VFN.cz a ve vztahu:

- k zaměstnancům: Informační memorandum pro zaměstnance,
- k pacientům: Informační memorandum pro pacienty.

3.1 POVĚŘENEC PRO OCHRANU OSOBNÍCH ÚDAJŮ VFN

VFN jako zpracovatel osobních údajů provádějící rozsáhlé zpracování má jmenovaného **Pověřence pro ochranu osobních údajů VFN** (také označovaný DPO), který zajišťuje tyto oblasti:

- nezávislá kontrolní a poradenská funkce ve vztahu k osobním údajům,
- sledování a vyhodnocení stavu souladu VFN s požadavky GDPR,
- komunikace se subjekty osobních údajů (pacienti, zaměstnanci) při využití jejich práv dle nařízení GDPR (např. právo na informaci, výmaz, námitku, přenositelnost),
- přijímání a spolupráce na vyhodnocení nahlášených případných incidentů narušení ochrany osobních údajů dle postupu definovaném v kapitole 4.6 Nahlášení podezření na únik OÚ,
- komunikace s Úřadem pro ochranu osobních údajů, nahlášení případných incidentů narušení ochrany osobních údajů,

[6] RD-VFN-04 Skartační řád

- ohlášení porušení ochrany osobních údajů dotčeným subjektům údajů.

Při potřebě vyjasnění, nesouladu, stížností nebo nahlášení incidentů (urgentních) ochrany osobních údajů je možné se obracet na pověřence pro ochranu osobních údajů VFN (dále také jen pověřenec) prostřednictvím kontaktního e-mailu: poverenec@vfn.cz.

4. Postup (popis činností)

4.1 ZÁSADY PRO PRÁCI S OSOBNÍMI ÚDAJI

1. K údajům, uvedeným ve zdravotnické dokumentaci pacientů smí mít **přístup** jenom osoby se způsobilostí k výkonu zdravotnického povolání a jiní odborní pracovníci v přímé souvislosti s poskytováním zdravotních služeb, kteří jsou zaměstnanci VFN, a další zaměstnanci v rozsahu nezbytně nutném a dále z důvodu splnění úkolů dle obecně závazných právních předpisů a při hodnocení správného postupu při poskytování zdravotních služeb (mají např. pověření interního auditora schválené ředitelem VFN).
2. **Nosiče dat** s osobními údaji (kartotéky, dokumenty, výpočetní technika, paměťová média…) musí být uschovány v prostorách zabezpečených proti vstupu neoprávněných osob. Odpovědné osoby jsou povinny kartotéky důsledně zamykat a nenechávat nosiče dat (i zdravotnickou dokumentaci) volně ležet. Chybné výtisky, kontrolní tisky apod. musí být skartovány tak, aby se nedaly osobní údaje přečíst, paměťová média a soubory musí být v lokálních stanicích vymazány.
3. V případě **předávání výpočetní techniky nebo zdravotnické techniky**, ve které jsou uloženy osobní údaje, do opravy nebo při vyřazení, je příslušný zaměstnanec povinen informovat zaměstnance Úseku informatiky (prostřednictvím ServiceDesku) a ti jsou povinni zamezit úniku osobních údajů.
4. **Místnosti**, v nichž je instalována výpočetní technika pracující s hromadnou úschovou dat (centrální serverovny), musí být zabezpečeny prvky aktivní i pasivní bezpečnosti v souladu se směrnicí SM-VFN-35 Zabezpečení a přístup do prostor (tj. chráněný vstup do místností, zabezpečení oken, protipožární signalizace) a zpracovávaná data zabezpečena softwarovými prostředky k ochraně dat a programů (přístupová hesla, antivirová ochrana, šifrování dat apod.).
5. **Přístup k lokálním stanicím**, na kterých jsou uloženy nebo zpracovávány osobní údaje, musí být znemožněn neoprávněným osobám např. povinností zadat heslo před jeho spuštěním.
6. Zaměstnanci nesmí na lokálních stanicích určených k uchovávání a zpracovávání osobních údajů používat **neautorizované programy** vč. výukových a demonstračních.
7. Správce ICT je povinen provádět pravidelné **zálohy** (bezpečnostní kopie dat uložených v elektronické podobě) a ukládat je v místnostech oddělených od místností, kde je instalována výpočetní technika a zabezpečit je proti odcizení. Nepotřebné nebo poškozené zálohy musí být zlikvidovány tak, aby nemohlo dojít k jejich zneužití.
8. Data obsahující osobní údaje, která jsou používána ke **studijním, vědeckým, statistickým účelům atd.**, musí být anonymizována, tedy **zbavena osobních údajů,** tj. identifikačních znaků (rodné číslo, jméno a příjmení, adresa,…).

Podrobně jsou pravidla pro nakládání s citlivými a osobními údaji popsána v Řádu používání informačních systémů (RD-VFN-11).

4.2 EVIDENCE, ZPRACOVÁNÍ, ULOŽENÍ A ZABEZPEČENÍ OÚ

V případě, že je na pracovišti prováděno **zpracování osobních údajů z jiného důvodu** (např. klinické studie, marketingový průzkum, apod.)**, než je dodržování obecně závazných právních předpisů, smluvních povinností, oprávněného zájmu VFN, je nezbytné** pro zpracování osobních údajů **získat souhlas subjektu osobních údajů**. Postup, povinnosti a požadavky na získání souhlasu jsou definované v kapitole 4.3 Souhlas se zpracováním osobních údajů.

Příslušný vedoucí zaměstnanec, který je odpovědný za rozhodnutí o sběru nebo ukládání osobních údajů, jeho změnu nebo skončení, je o této skutečnosti povinen **před provedením změny zadat požadavek na zpracování osobních údajů do ServiceDesku a vyplnit formulář** (F-VFN-445), který je přiložen do požadavku.

Odpovědný zaměstnanec ÚI za Registr zpracování osobních údajů VFN (dále jen Registr OÚ) provede následující kroky:

- na základě zadaného požadavku a dodaných informací ve formuláři (F-VFN-445), posoudí úplnost a srozumitelnost dodaných informací. Struktura požadovaných informací je uvedena v následujících bodech:
  - architekturu/popis řešení,
  - popis procesu nakládání s osobními údaji,
  - místo uložení a zabezpečení osobních údajů,
  - způsob přístupu k osobním údajům,
  - komu a jak jsou předávány osobní údaje,
  - stanovit vlastníka, garanta a správce celého řešení nebo jeho komponent,
  - smluvní náležitosti (pokud je to relevantní),
  - rozsah zpracovávaných údajů, hlavně osobních a citlivých údajů,
  - apod.
- v případě neúplnosti dodaných informací je požadavek prostřednictvím ServiceDesku vrácen žadateli k doplnění,
- kompletní informace nebo požadované změny ve zpracování osobních údajů jsou zaznamenány do Registru OÚ, který udržuje ÚI v aktuálním stavu,
- v případě, že žadatel oznamuje v registračním formuláři (F-VFN-445) zpracování nových, změněných nebo ukončení zpracování osobních údajů na lokálním HW nebo SW k registraci, je současně provedeno zaznamenání HW a SW do evidence ÚI do databáze admincentrum.vfn.cz,
- po zaznamenání do Registru OÚ je prostřednictvím ServiceDesku zaslána žadateli informace o vyřešení požadavku a při novém zpracování lze osobní údaje k danému účelu zpracovávat.

4.3 SOUHLAS SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ

Ke zpracování osobních údajů je potřeba souhlas subjektu údajů pouze v případě, že zpracování osobních údajů neprovádí VFN na základě zákona, povinností vyplývajících ze smlouvy nebo z důvodu oprávněného zájmu. Účely, pro které VFN osobní údaje zpracovává, lze rozdělit do následujících hlavních okruhů:

- plnění smlouvy,
- služby pro zaměstnance nad rámec pracovně právního vztahu,

- řízení rizik,
- zajišťování bezpečnosti včetně plnění právních povinností VFN jako zaměstnavatele a poskytovatele zdravotních služeb, vnitřní správa včetně rozvoje a zlepšování služeb.

V případě souhlasu se zpracováním osobních údajů je poskytnutí osobních údajů pro účely definované v daném souhlasu vždy zcela na úvaze zaměstnance, pacienta nebo jiného subjektu ve vztahu k VFN.

Souhlas se zpracováním osobních údajů pacienta, zaměstnance nebo případně další osoby musí splňovat následující podmínky, tj. být:

- svobodně udělený (pokud není udělen, nesmí být znevýhodněn),
- informovovat o účelu a rozsahu souhlasu,
- srozumitelně a jednoznačně formulován,
- zřetelně oddělen od jiného textu,
- kdykoliv odvolatelný stejně snadno, jako byl dán.

Osobní údaje zpracovávané na základě souhlasu subjektu osobních údajů, jsou zpracovávány po dobu, na kterou je souhlas udělen, resp. do okamžiku, než subjekt údajů svůj souhlas odvolá. Je nezbytné zajistit správcem údajů (zpravidla VFN) schopnost doložit udělení souhlasu.

Při získání souhlasu pro VFN musí být dodržen následující postup:

- odsouhlasení obsahu LPO,
- zajištění svobodného souhlasu od subjektu,
- uložení souhlasu do bezpečného úložiště,
- datové úložiště souhlasů nebo papírové souhlasy musí být chráněny proti neoprávněnému přístupu, odcizení a jakékoliv poškození integrity nebo věrohodnosti,
- sledování provedených změn, odvolání nebo smazání/skartace po celou dobu platnosti souhlasu,
- dodržení skartační lhůty.

4.4 ZADÁNÍ POŽADAVKU SUBJEKTU VYPLÝVAJÍCÍ Z JEHO PRÁV

Pacient nebo zaměstnanec (stejně jako další osoby) má nárok dle práv definovaných v GDPR:

- na podání žádosti na informace o zpracovávaných osobních údajích,
- na podání žádosti na opravu osobních údajů,
- na podání žádosti na výmaz osobních údajů,
- na vznesení námitky proti zpracování svých osobních údajů,
- na podání žádosti na přenositelnost zpracovávaných osobních údajů,
- na podání žádosti nebýt předmětem automatizovaného individuálního rozhodování, včetně profilování,
- apod.

a zadá svůj požadavek:

- Zaměstnanec (v pracovním poměru):
    - zašle z pracovního e-mailu (jméno.příjmení@vfn.cz) na adresu poverenec@vfn.cz;
- Pacient, bývalý zaměstnanec, stejně jako další osoby:

- zašle poštou na adresu VFN: písemně s úředně ověřeným podpisem žadatele,
- osobním doručením žádosti do podatelny VFN, následně v procesu vyřízení žádosti bude ověřena totožnost žadatele,
- zašle e-mailem na adresu poverenec@vfn.cz, kterou podepíše vlastním platným kvalifikovaným elektronickým podpisem,
- zašle datovou schránkou, kdy se žadatel musí shodovat s odesílatelem datové zprávy.

4.5 NAHLÁŠENÍ PODEZŘENÍ NA PORUŠENÍ ZABEZPEČENÍ OÚ

V případě **podezření nebo zjištění porušení zabezpečení osobních údajů**, tj. takového, které může vést k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů (např. nesprávně zaslaný e-mail, ztracená USB Flash, odcizená nebo ztracená zdravotnická dokumentace apod.), zadá každý zaměstnanec tuto skutečnost neprodleně:

- do ServiceDesku kategorie Incident/Bezpečnostní incident/**Únik osobních údajů**,
- nebo **v neodkladných případech nahlásí pověřenci** pro ochranu osobních údajů na adresu poverenec@vfn.cz, aby byly minimalizovány dopady incidentu na vnitřní IS VFN nebo zabráněno eskalaci negativních jevů vně VFN.

4.6 VYHODNOCENÍ A OHLÁŠENÍ PORUŠENÍ ZABEZPEČENÍ OÚ

Po nahlášení podezření na porušení zabezpečení osobních údajů do ServiceDesku nebo oznámení pověřenci pro ochranu osobních údajů je nezbytné zajistit následující kroky:

- vyhodnocení podezření, zda se jedná o porušení zabezpečení OÚ, o jeho rozsahu a následné kroky,
- při porušení zabezpečení osobních údajů zajistit:
  - ohlášení porušení Úřadu pro ochranu osobních údajů,
  - ohlášení porušení dotčeným subjektům údajů,
  - posouzení rizik spojených s porušením.

Postup je dále upřesněn v příloze (Příloha č. 2Příloha č. 2 - Vyhodnocení a ohlášení porušení zabezpečení OÚ) této směrnice.

4.7 ZPRACOVÁNÍ MIMO ČESKOU REPUBLIKU

Při zpracování v rámci Evropského hospodářského prostoru („EHP“) **platí** režim volného pohybu osobních údajů a pro jejich zpracování se uplatní **stejná pravidla jako v České republice**.

V případech, kdy smluvní partneři VFN zpracovávají osobní údaje ve třetích zemích (tedy zemích mimo EHP), musí být informace o zpracování mimo EHP zadána při nahlášení nebo změně zpracování osobních údajů dle postupu definované v kapitole 4.2 Evidence, zpracování, uložení a zabezpečení OÚ a to vždy při dodržení veškerých legislativních požadavků. Pokud dochází ke zpracování osobních údajů v USA, musí být dodrženy požadavky v rámci tzv. programu Privacy Shield („Štít soukromí“) včetně registrace nebo garantovány obdobné záruky vysoké ochrany osobních údajů (např. tzv. standardní smluvní doložky).

4.8 KAMEROVÉ SYSTÉMY

Provozování kamerového systému je považováno za formu zpracování osobních údajů, v případě, že je vedle kamerového sledování prováděn i záznam pořizovaných záběrů.

Kamerový systém může být provozován z důvodů **ochrany majetku VFN, zdraví a života** pacientů, zaměstnanců a návštěvníků VFN.

Technický správce kamerového systému (Úsek informatiky) vede seznam všech kamer zapojených v systému, včetně jejich umístění, režimu provozu, popisu, důvodu provozování, lhůty pro výmaz záznamu, HW konfigurace a pohledového snímku jednotlivých kamer.

V případě žádosti o instalaci kamer nebo monitorování prostor musí být:

- zadán požadavek na zpracování osobních údajů do ServiceDesku a vyplněn formulář (F-VFN-445), který je přiložen k požadavku,
- v případě neúplnosti dodaných informací je požadavek prostřednictvím ServiceDesku vrácen žadateli k doplnění,
- požadavek je předán pověřenému pracovníkovi Útvaru bezpečnosti a krizové připravenosti k posouzení potřeby a případného umístění kamery ke schválení,
- po schválení je zajištěno ÚI nainstalování kamery.

Technické podmínky, postup a pravidla pro provozování kamerového systému a pořizování, uchování a správu audiovizuálních dat z tohoto systému v areálu a objektech VFN v souladu s platnou legislativou vztahující se k ochraně osobních údajů, osoby používající kamerový systém, jejich povinnosti, odpovědnost a pravomoci jsou definovány v řádu Provozování kamerového systému ve VFN (RD-UI-10).

5. Závěrečná ustanovení

Porušení ochrany osobních údajů bude posuzováno jako závažné porušení povinností vyplývajících z právních předpisů vztahujících se k zaměstnancem vykonávané práci a jednání v rozporu se zájmy VFN jako zaměstnavatele.

6. Vznikající dokumenty a údaje

Název	Uchovává	Doba uchování

7. Související dokumenty

RD-VFN-01 Léčebný řád VFN
RD-VFN-11 Používání informačních systémů
RD-VFN-04 Skartační řád
RD-VFN-04P Spisový a skartační plán dokumentů
SM-VFN-35 Zabezpečení a přístup do prostor
F-VFN-445 Nahlášení/změny/ukončení zpracování osobních údajů

RD-UI-10 Provozování kamerového systému ve VFN

Informační memorandum pro zaměstnance

Informační memorandum pro pacienty

Legislativa (v platném znění):
Zákon č. 101/2000 Sb., o ochraně osobních údajů;
Zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování;
Nařízení Evropského parlamentu a Rady (EU) č. 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 (obecné nařízení o ochraně osobních údajů); neboli GDPR (General Data Protection Regulation);
Stanovisko ÚOOÚ č. 6/2012 Zpracování osobních údajů zaměstnanců;
Stanovisko ÚOOÚ č. 3/2015 Zpracování osobních údajů v souvislosti s vedením zdravotnické dokumentace.

8. Přílohy

8.1 PŘÍLOHA Č. 1

Příloha č. 1 - Smluvní náležitosti ochrany osobních údajů

8.2 PŘÍLOHA Č. 2

Příloze č. 2 - Vyhodnocení a ohlášení porušení zabezpečení OÚ