**3. Popis modelové ordinace (minimální standardy zabezpečení osobních údajů)**

**Výklad**

Tato část obsahuje popis minimálních standardů zabezpečení osobních údajů tak, jak vyplývají z aktuálně platných právních předpisů. Nejde o povinnou součást dokumentace správce osobních údajů.

Z uvedených standardů jsme vycházeli při zhodnocení míry pravděpodobnosti jednotlivých hrozeb v tabulce č. 2. Konkrétní metody a opatření, jak dosáhnout uvedených standardů, popisuje směrnice uvedená dále v části 4.

Lze s jistou mírou zobecnění říci, že poskytovatel, který nesplňuje uvedené standardy, nebude schopen zajistit soulad zpracování osobních údajů s GDPR. Projeví se to i v tabulkové části. Pokud nesplňujete minimální standardy, poctivě vyhodnotíte míru pravděpodobnosti hrozeb a do tabulky č. 2 (třetí sloupec) uvedete odpovídající hodnoty, ukáže Vám tabulka č. 3, že rizika z dotčených zpracování nejsou přijatelná. Lze proto doporučit, aby každý poskytovatel minimální standardy popsané v této části dodržoval.

**Minimální standardy zabezpečení osobních údajů v ambulanci**

Při tvorbě vzorových dokumentů bylo nutno vycházet z modelové ordinace, která již v současné době věnuje ochraně osobních údajů dostatečnou pozornost a má nastaveny určité provozní standardy (tj. předpokládá se soulad s požadavky zákona č. 101/2000 Sb., o ochraně osobních údajů a zákona č. 372/2011 Sb., o zdravotních službách). Od těchto standardů se pak odvíjí hodnocení rizik a pravděpodobnosti jejich výskytu v předkládaných dokumentech. Současně je nutno brát v potaz, že každá ordinace je určitým způsobem specifická a tato specifika by se měla v hodnoceních odrazit (např. vede dokumentaci elektronicky, má různé objednávkové systémy atp.).

S ohledem na různé typy a způsoby zpracování osobních údajů jsme vycházeli z následujícího:

**Zabezpečení ordinace:**

Přístupové dveře do ordinace jsou uzamykatelné a neumožňují vstup do ordinace bez přítomnosti personálu poskytovatele. Na místech veřejně přístupných (čekárny, chodby) nejsou skladovány dokumenty obsahující osobní údaje (např. v čekárně není kartotéka); pokud tomu tak je, jsou místa, kde jsou dokumenty skladovány, uzamykatelná a pod stálým dohledem personálu poskytovatele.

**Vedení a nakládání s dokumentací:**

Při vedení dokumentace v listinné podobě je k ní zajištěn pouze zabezpečený přístup a po vyjmutí karty pacienta z kartotéky je karta přístupná pouze lékaři a sestře, příp. další osobám podle příslušných ustanovení zákona č. 372/2011 Sb.; karta je následně ihned uložena zpět do kartotéky.

V případě elektronického vedení dokumentace je zajištěna ochrana dat prostřednictvím hesla a jednoznačné identifikace uživatele při jeho přístupu k datům. Poskytovatel používá legálně získaný, výrobcem podporovaný a aktualizovaný software (operační systém i program pro vedení zdravotnické dokumentace) a jeho výpočetní technika je vybavena alespoň základním bezpečnostním programem (antivirový software).

Veškeré nakládání se zdravotnickou dokumentací probíhá podle příslušných ustanovení zákona č. 372/2011 Sb., tj. nahlížení, pořizování kopií a výpisů je umožněno pouze oprávněným osobám.

**Uchovávání dokumentace:**

Dokumentace v listinné podobě je uchovávána v uzamykatelné kartotéce nebo je pod stálým dohledem personálu poskytovatele.

V případě elektronického vedení dokumentace jsou splněny požadavky zákona č. 372/2011 Sb.

**Objednávací systém:**

Objednávací systém je veden tak, aby byl přístupný pouze personálu poskytovatele.

**Osobní spisy zaměstnanců:**

Jsou uloženy na zvláštním místě a přístup k nim má pouze poskytovatel.

Veškeré další dokumenty obsahující osobní údaje jsou přístupné pouze poskytovateli, jeho zaměstnancům nebo osobám k tomu určeným.