



GDPR

Dopady na datový management diabetu

Od 25. května 2018 platí přísné předpisy Obecného nařízení o ochraně osobních údajů (GDPR). Porušení zabezpečení ochrany osobních údajů bude v budoucnu trestáno citelnými pokutami.

Nové předpisy mají rovněž masivní dopady na digitální management diabetu. Aktuálně dostupná řešení skýtají s ohledem na ochranu osobních dat různá rizika a povinnosti.

**Informace
na druhé straně**

Od 25. května 2018 platí přísné předpisy Obecného nařízení o ochraně osobních údajů (GDPR).

Při porušení zabezpečení ochrany osobních údajů nebo nedodržení zákonných povinností hrozí citelné pokuty.

Nové předpisy mají rovněž masivní dopady na digitální management diabetu.

Takováto řešení jsou k dostání buď jako lokálně ukládaný software nebo jako internetová „cloudová“ aplikace.

Z hlediska požadavků na ochranu osobních údajů se tato řešení značně liší:

Spíše neproblematická zůstávají i nadále řešení, kdy žádná z dat neopustí ordinaci/kliniku.

Pokud jsou však patientská data posílána do „cloudu“ (= výrobci/třetí osobě), pak byste si měli být vědomi značných rizik a nákladů, které je nutné vynaložit na užívání v souladu se zákonem.

Co mnoho ordinací neví: při použití cloudového řešení je zpravidla nezbytné jmenovat pověřence pro ochranu osobních údajů** – a sice nezávisle na počtu zaměstnanců!

DIABASS® PRO (lokální aplikace)



Všechna data jsou uložena lokálně;
žádná data nejsou zasílána třetím osobám.

- není nutné zvláštní poučení
- není nutný zvláštní souhlas
- žádné požadavky, které by překračovaly stávající povinnosti v souladu s ochranou osobních údajů
- žádné nebezpečí trestního postihu podle § 203 trestního zákoníku
- není potřeba připojení k internetu
- není zapotřebí pověřence pro ochranu osobních údajů
- žádná závislost na třetích osobách
- snadné vytvoření/obnovení záloh
- snadné splnění archivačních a dokumentačních povinností v souladu se zákonem díky lokální úschově
- není nutný outsourcing dat: i velké datové soubory se vejdou na běžný USB flash disk*

* Příklad výpočtu: 2000 pacientů s údaji CGM po dobu 10 let, požadavky na kapacitu paměti = cca 30–50 GB

Webové aplikace („cloud“)



Pacientská data jsou zasílána výrobcům zařízení, resp. třetím osobám a zde jsou ukládána. Tyto osoby mohou do dat nahlížet a (spolu)užívat je.

- předpisy vyžadují jmenování pověřence pro ochranu osobních údajů (i u ordinací s < 10 zaměstnanci!)**
- je nutné obsáhlé poučení pacienta
- je nutný informovaný souhlas pacienta
- přenos dat musí být i z lékařského hlediska nutný (čl. 5 odst. 1 písm. b) GDPR)
- vysoké nebezpečí trestního postihu podle § 203 trestního zákoníku
- při nefunkčním připojení internetu / nedostupnosti: nelze pracovat
- vytvoření/obnova záloh závisí na poskytovateli a/ nebo je časově náročná
- zákonem předepsané archivační a dokumentační povinnosti lze jen stěží splnit
- potenciální spoluzodpovědnost při porušení zabezpečení ochrany osobních údajů ze strany poskytovatele
- dodávání patientských dat výrobcům je z hlediska profesní legislativy a zákonů o hospodářské soutěži problematické
- jen stěží slučitelné s doporučeními Spolkové lékařské komory

** 38 odst. 1 str. 2 spolkového zákona na ochranu dat, resp. nařízení úřadů pro ochranu dat ze dne 17. 10. 2018, č. 15, (https://www.lda.bayern.de/media-dsfa_muss_liste_dsk_de.pdf)



DIABASS® PRO nabízí bezpečnost: všechny údaje zůstávají uloženy výhradně u lékaře. Žádné údaje o pacientech nebo užívání nejsou posílány do „cloudu“ nebo výrobcům.

Z hlediska práva na ochranu dat není zapotřebí zohlednit nic zvláštního, co by přesahovalo stávající povinnosti v oblasti ochrany osobních údajů v ordinaci.

Na rozdíl od tzv. „cloudových“ řešení tedy není nutné pacienty poučovat o předávání dat a předem zajišťovat právně bezpečné souhlasy. Využití **DIABASS® PRO** navíc nevyžaduje ani jmenování pověřence pro ochranu osobních údajů.



Nová verze DIABASS® PRO nejenže lékaři ušetří správní náklady a minimalizuje riziko pokut, ale zároveň jej podporuje při plnění obecných povinností v souvislosti se zákonem na ochranu dat. Jedním stisknutím tlačítka lze například vytvořit souhrnnou informaci o osobních údajích pacienta (podle čl. 15 GDPR) nebo na jeho žádost vystavit strukturovanou kopii údajů (podle čl. 20 GDPR).