Aplikace pseudonymizační techniky ve zdravotnictví

Typ dokumentu: Studie

Autor: Evropská agentura pro kybernetickou bezpečnost

Datum: (24. března 2022)

Zdroj: Tisková zpráva

Shrnutí

Vzhledem k tomu, že se oblast zdravotnictví usiluje o co nejlepší využití vyvíjejícího se technické prostředí a přizpůsobení poskytování služeb tak, aby včas naplnilo rostoucí potřeby pacientů, přicházejí do hry další výzvy v oblasti kybernetické bezpečnosti a ochrany údajů.

Díky velkému objemu dat má zdravotnický sektor kapacitu zlepšit diagnostiku a modelování klinických výsledků, pomoci vyhodnotit strategie včasné intervence atd. Tento nový ekosystém zlepšuje poskytování a monitorování zdravotnických služeb na různých úrovních včetně rozhodování a poskytuje včasnou, vhodnou a nepřerušovanou lékařskou péči.

Technologický pokrok ve zdravotnictví tvoří rostoucí poptávku po velkých lékařských databankách, které by nabízely řešení například v oblasti diagnostiky onemocnění a fenotypizace, modelování klinických výsledků, predikce strategií časné intervence, precizní medicíny atd. Rostoucí objem zpracování digitalizovaných lékařských údajů však současně zvyšují rizika, pokud jde o kybernetickou bezpečnost, ochranu údajů a pravděpodobnost narušení údajů.

Ochrana zdravotních údajů je považována za vysokou prioritu vzhledem k jejich citlivé povaze a dopadu, který mají na jednotlivce (subjekty údajů). Z hlediska kybernetické bezpečnosti je důvěrnost, dostupnost a integrita lékařských údajů a příslušné infrastruktury považována za zásadní k tomu, aby bylo možné poskytovat včasnou, vhodnou a nepřerušovanou lékařskou péči.

Kvůli rostoucí potřebě vyměňovat si a sdílet informace o zdraví jednotlivců mezi různými zúčastněnými stranami je nezbytné, aby subjekty zpracovávající osobní údaje na jedné straně shromažďovaly a dále zpracovávaly pouze údaje, které jsou nezbytné pro jejich účely, a na straně druhé uplatňovaly řádná organizační a technická opatření k ochraně těchto osobních údajů.

Zpráva vysvětluje, jak lze techniky použít ke zlepšení úrovně ochrany osobních údajů prostřednictvím jednoduchých případů použití. Rozhodnutí o technikách, které mají být použity, by mělo být založeno na dříve provedených činnostech hodnocení dopadu rizik, jako jsou:

- Cílové osobní údaje (např. soubor identifikátorů);
- Technika, která má být použita;
- Parametry použitelné pro danou techniku;
- Politiku pseudonymizace, která se má použít.

Techniky a parametry, které je třeba vzít v úvahu, se proto mohou lišit podle platných požadavků ve vztahu k předpisům, rychlosti, jednoduchosti, předvídatelnosti a nákladům.

Scénáře zvolené pro prozkoumání těchto parametrů jsou:

- Výměna zdravotních údajů pacienta;
- Klinické testy;
- Monitorování zdravotních údajů ze zdrojů pacienta.

GDPR definuje pseudonymizaci v čl. 4 odst. 5 jako: „zpracování osobních údajů takovým způsobem, že osobní údaje již nelze přiřadit konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a podléhají technickým a organizačním opatřením, aby bylo zajištěno, že osobní údaje nebudou přiřazeny identifikované nebo identifikovatelné fyzické osobě“.

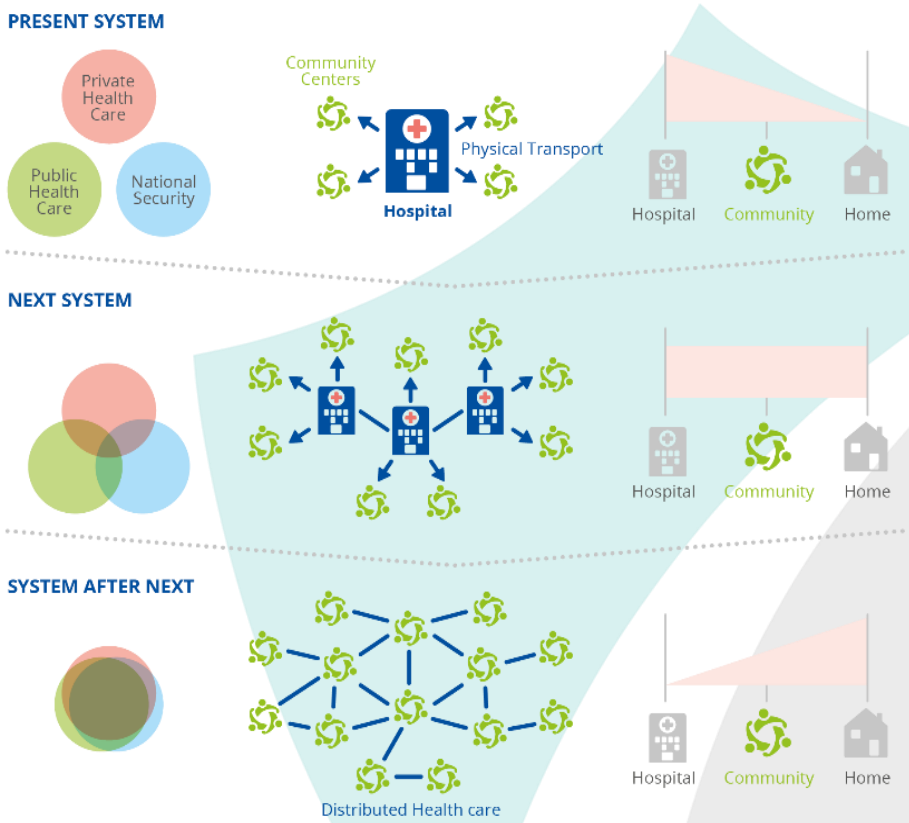
Pseudonymizace se stále více stává klíčovou bezpečnostní technikou pro poskytování prostředků, které mohou usnadnit zpracování osobních údajů a zároveň nabízejí silné záruky ochrany osobních údajů, a tím chrání práva a svobody jednotlivců. Cílem pseudonymizace je chránit osobní údaje skrytím identity jednotlivců v datové sadě, např. nahrazením jednoho nebo více osobních identifikátorů tzv. pseudonymy (a vhodnou ochranou spojení mezi pseudonymy a původními identifikátory).

Hlavní výhodou pseudonymizace při správné aplikaci je skrytí identity jednotlivce v kontextu konkrétního datasetu, takže není možné spojit data s konkrétní osobou. Proto může také snížit riziko propojení osobních údajů u konkrétního jednotlivce napříč různými doménami zpracování údajů.

Přehled základních pseudonymizačních technik:

Technika	Generátoru pseudonymů
Počítadlo	Monotónní počítadlo, které začíná na určité hodnotě a je zvýšeno pokaždé, když je nutný nový pseudonym.
Náhodné číslo	Náhodná hodnota extrahovaná mezi minimální a maximální hranicí pokaždé, když je nutný nový pseudonym.
Hašovací funkce	Jednosměrná (nevratná) kryptografická funkce transformující vstupní osobní data na hodnoty s pevnou délkou.
Hašovací kód pro ověření zprávy (HMAC)	Jednosměrná (nevratná) kryptografická funkce přidání klíče, díky kterému je méně předvídatelná než hašovací funkce.
Šifrování	Obousměrná (reverzibilní) kryptografická funkce transformující vstupní osobní údaje na hodnoty, které lze pomocí klíče znovu transformovat do původního formátu.

Z grafiky zprávy



(Digitální transformace vyvolala posun hodnoty ve zdravotnictví.)