Kybernetická bezpečnost ve zdravotnictví

Poskytovatelé zdravotní péče zatím nejsou v naprosté většině regulováni zákonem o kybernetické bezpečnosti. Připravovaná směrnice NIS 2 změní pravidla působnosti zákona o kybernetické bezpečnosti a při tom i sníží hranici pro velikost poskytovatele zdravotní péče, na kterého se bude zákon vztahovat. Spolu s dalším připravovaným nařízením Evropské komise o European Health Data Space zásadně zvýší nároky na kybernetickou bezpečnost elektronických dat pořizovaných poskytovateli zdravotní péče.

Právní regulace kyberbezpečnosti ve zdravotnictví vychází ze zákona č. 181/2014 Sb., o kybernetické bezpečnosti. Dále je kodifikuje směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016, o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (NIS). Kybernetickou bezpečnost elektronických záznamů pořizovaných při poskytování zdravotní péče pak v blízké budoucnosti zásadně upraví návrh Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o zrušení směrnice (EU) 2016/1148 (NIS 2).

Publikace finálního znění směrnice NIS2 se předpokládá ve čtvrtém čtvrtletí roku 2022. Transpoziční lhůta (tj. lhůta, ve které musí členské státy směrnici promítnout do národního práva) je stanovena na 21 měsíců. Z toho plyne, že pokud se výše zmíněný předpoklad naplní, přibližně v polovině roku 2024 by Česká republika měla mít zaveden nový rámec povinností v národní legislativě (formou novelizace zákona o kybernetické bezpečnosti a některých dalších relevantních předpisů). Další lhůta pak bude stanovena pro zahájení plnění nových povinností u těch organizací, které dosud regulaci kybernetické bezpečnosti nepodléhaly. Podle NIS2 nově povinné subjekty již nebude Národní úřad pro kybernetickou a informační bezpečnost jako dosud informovat (určovat), že vstupují do regulace, ale budou si muset sami vyhodnotit, zda splňují kritéria povinných subjektů. Nová regulace kyberbezpečnosti ve spojení se stávající už tak dost přísnou regulací ochrany osobních údajů dle GDPR může být v budoucnu ještě umocněna přijetím zákona o hromadném řízení (žalobách), který připravuje vláda ČR a který bude aplikovatelný mimo jiné třeba i na případy úniků citlivých dat pacientů..

3. května 2022 byl zveřejněn Evropskou komisí legislativní balíček s návrhem Nařízení na téma Evropského prostoru pro zdravotní data (EHDS), který bude mít zásadní význam pro digitalizaci zdravotnictví, podporu poskytování zdravotní péče, ale také pro výzkum v oblasti zdraví a tvorbu zdravotní politiky.

Záměrem EHDS nařízení je umožnit pacientům přístup ke svým zdravotním údajům a získat nad nimi kontrolu. Pacient bude mít rychlý a bezpečný přístup ke svým údajům/datům. Bude mít možnost udělení souhlasu či naopak zákazu využití jeho dat pro poskytnutí zdravotní péče (ze strany zdravotnických pracovníků a lékárníků). Bude moci doplňovat data do svého elektronického záznamu. Nařízení nastaví právní rámec a zavede infrastrukturu pro výměnu různých druhů zdravotních údajů jak pro primární využití dat (využití za účelem poskytování zdravotní péče), tak sekundární využití dat (využití pro účely výzkumu, inovací, tvorby politik, regulaci, návrh modelů personalizované péče). EHDS má dále posílit dosavadní model spolupráce a správy v oblasti zdravotních dat na úrovni členských států i EU a podpořit vznik jednotného trhu relevantních ICT technologií v EU.

Návrh Nařízení o EHDS přímou povinnost jednotlivým zdravotnickým pracovníkům vést zdravotnickou dokumentaci v elektronické podobě v tomto znění neukládá. Nicméně nařízení obsahuje mnohá práva fyzických osob v přístupu k elektronické zdravotní dokumentaci. Občané členských států EU budou například mít po zavedení EHDS právo poskytnout přístup k údajům ze sektoru zdravotnictví nebo požádat držitele údajů ze sektoru zdravotního o předání svých elektronických zdravotních údajů příjemci údajů ze sektoru zdravotnictví dle vlastního výběru. A to okamžitě, bezplatně a bez překážky ze strany držitele údajů nebo výrobců systémů používaných tímto držitelem. Implementace nařízení také předpokládá certifikaci softwarů a aplikací zpracovávajících elektronické zdravotní údaje.

Nové legislativní požadavky na bezpečnost a dostupnost zdravotních údajů budou klást velké implementační nároky především na poskytovatele primární péče. Většina kontaktů pacienta s poskytovateli zdravotní péče probíhá v ordinaci praktického lékaře. Praktici zároveň jako jediní poskytovatelé péče spravují i zdravotní data zdravých občanů. Na rozdíl od nemocnic, ale nemají k dispozici podporu žádného GDPR pověřence ani IT oddělení. Většina zdravotníků v primární péči jsou ženy a ICT compliance je nízko na žebříčku jejich profesních zájmů. Více než 50% praktických lékařů nemá k dispozici žádného ICT specialistu. Digitalizace zatím neúměrně zvyšuje administrativní zátěž praktického lékaře při poskytování zdravotní péče. Příkladem je nutnost uvádět 51 údajů při vystavení e-neschopenky nebo e-vakcinace.

Ochrana dat ve zdravotnictví musí být podřízena primární funkci zdravotnictví tedy poskytování zdravotní péče. Lékařům musí zůstat zachován prostor pro záznam poznámek o pacientovi které s ním nebudou sdíleny. Povinnost implementovat zvyšující se nároky na kybernetickou bezpečnost ve zdravotnictví by měli mít především poskytovatelé ICT řešení nikoliv poskytovatelé péče. Připravované povinné certifikace softwarů a aplikací zpracovávajících elektronické zdravotní údaje by se měli vyhnout riziku monopolizace dodavatelské infrastruktury v situaci, kdy malé společnosti nedosáhnou na nákladnou certifikaci.

Aby lékaři v primární péči podporovali implementaci kybernetické bezpečností je zapotřebí kvalitní profesní vzdělávání v nových povinnostech. Lékaři by měli být u vzniku ICT systémů od začátku, aby vzniklá řešení reflektovala potřeby a možnosti praxe. Primární péče bude potřebovat dotační podporu při implementaci narůstajících nároků na kybernetickou bezpečnost. Tato podpora by mohla být realizována formou dotačních šablon, které se osvědčily v distribuci dotačních prostředků a funkčních řešení odpovídajících rozdílným potřebám příjemců podpory v digitalizaci školství.