

Zdravotnická informatika – Směrnice pro ochranu přeshraničních toků osobních zdravotních údajů

ČSN
ISO 22857
98 0024

Health informatics – Guidelines on data protection to facilitate transborder flow of personal health data

Informatique de santé – Lignes directrices sur la protection des données pour faciliter les flux d'information sur la santé
du personnel de part et d'autre des frontières

Tato norma je českou verzí mezinárodní normy ISO 22857:2013. Překlad byl zajištěn Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO 22857:2013. It was translated by the Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Národní předmluva

Souvisící ČSN

ČSN EN ISO 27799 (98 2021) Zdravotnická informatika – Systémy řízení bezpečnosti informací ve zdravotnictví využívající ISO/IEC 27002

ČSN P CEN ISO/TS 14265 (98 1038) Zdravotnická informatika – Kategorie třídění dat při zpracování osobních zdravotních informací

ČSN EN ISO 21091 (98 2023) Zdravotnická informatika – Služby adresáře pro poskytovatele zdravotní péče, subjekty péče a ostatní entity

ČSN EN ISO 27789 (98 2025) Zdravotnická informatika – Auditní záznamy elektronických zdravotních záznamů

Vysvětlivky k textu převzaté normy

- 1) Anglický termín „safety“ je pro účely této normy překládán jako „bezpečnost“ nebo „ochranné opatření“ dle významu.
- 2) Anglický termín „transfer“ je pro účely této normy překládán jako „předání“ dle právního výkladu.

Vypracování normy

Zpracovatel: Ing. Jindřich Kodl, CSc., IČ 63957108

Technická normalizační komise: TNK 20 Informační technologie

Pracovník Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Ing. Miroslav Škop

MEZINÁRODNÍ NORMA

Zdravotnická informatika – Směrnice pro ochranu ISO 22857
přeshraničních toků osobních zdravotních údajů Druhé vydání
2013-12-15

ICS 35.240.80

Obsah

Strana

Předmluva 7

Úvod 8

1 Předmět normy 10

2 Citované dokumenty 10

3 Termíny a definice 10

4 Zkrácené termíny 12

5 Struktura této mezinárodní normy 12

6 Obecné principy a role 12

6.1 Obecné principy 12

6.2 Role 13

7 Legitimizace předání údajů 13

7.1 Pojem „přiměřená“ ochrana údajů 13

7.2 Podmínky pro legitimní předání 14

8 Kritéria pro zajištění přiměřené ochrany údajů v souvislosti s předáním osobních zdravotních údajů
14

8.1 Požadavek na přiměřenou ochranu údajů 14

8.2 Obsah principů 14

8.3	Procesní/donucovací mechanismy	16
8.4	Smlouvy	18
8.5	Nadřazené právní předpisy	18
8.6	Anonymizace	18
8.7	Legitimita souhlasu	19
9	Bezpečnostní politika	19
9.1	Obecně	19
9.2	Účel bezpečnostní politiky	20
9.3	„Úroveň“ bezpečnostní politiky	20
9.4	Bezpečnostní politika na vysoké úrovni: obecné aspekty	20
10	Globální bezpečnostní politika: obsah	21
10.1	Princip jedna: Princip obecné nadřazenosti	21
10.2	Princip dvě: podpora vedoucího organizace	22
10.3	Princip tři: dokumentování opatření a přezkoumání	22
10.4	Princip čtyři: úředník pro ochranu bezpečnosti údajů	22
10.5	Princip pět: povolení ke zpracování	23
10.6	Princip šest: informace o zpracování	24

Strana

10.7	Princip sedm: informace pro subjekt údajů	26
10.8	Princip osm: zákaz dalšího předávání údajů bez souhlasu	26
10.9	Princip devět: opravné prostředky a náhrady	27
10.10	Princip deset: bezpečnost zpracování	27
10.11	Princip jedenáct: odpovědnosti personálu a ostatních dodavatelů	28
11	Odůvodnění a připomínky k opatřením, která podporují princip deset týkající se bezpečnosti zpracování	29
11.1	Obecně	29
11.2	Šifrování a digitální podpisy dovozců údajů pro přenos po sítích	29
11.4	Auditní záznamy	30

11.5 Fyzická bezpečnost a bezpečnost prostředí 30

11.6 Správa aplikace a správa sítě 30

11.7 Škodlivý software 30

11.8 Narušení bezpečnosti 30

11.9 Plán kontinuity činnosti organizace 30

11.10 Nakládání s velmi citlivými údaji 30

11.11 Normy 31

12 Osobní zdravotní údaje v neelektronické formě 31

Příloha A (informativní) Klíčové primární mezinárodní dokumenty o ochraně údajů 32

A.1 Směrnice EU o ochraně údajů 32

A.1.2 Zaměření 32

A.1.3 Pravidla pro zákonnost zpracování 32

A.1.4 Speciální kategorie zpracování 32

A.1.5 Práva subjektu údajů 33

A.1.6 Bezpečnost zpracování 33

A.1.7 Orgány dohledu 33

A.1.8 Opravné prostředky a sankce 33

A.1.9 Předávání osobních údajů třetím státům 34

A.2 Organizace pro hospodářskou spolupráci a rozvoj (OECD) 34

A.3 Rada Evropy 34

A.4 Valné shromáždění Spojených národů 35

A.4.1 Obecně 35

A.4.2 Principy týkající se minimálních záruk, které mají být stanoveny v jakýkoliv národních právních předpisech 35

A.4.3 Uplatnění pokynů pro soubory osobních údajů udržovaných vládními mezinárodními organizacemi 35

Příloha B (informativní) Národní dokumentované požadavky a právní předpisy v řadě států 36

B.1 Austrálie 36

B.2 Kanada 36

B.3 Evropa 38

B.4 Japonsko 38

B.5 Nový Zéland 38

B.6 Velká Británie 39

B.7 USA 39

Strana

Příloha C (informativní) Vzorová smluvní ustanovení: Od správce ke správci 40

C.1 Úvod 40

C.2 Atributy 40

C.3 Základní rysy smlouvy 40

C.4 Vzor smlouvy: poznámky 40

Příloha D (informativní) Vzorové smluvní doložky: Od správce ke zpracovateli 46

D.1 Úvod 46

D.2 Atributy 46

D.3 Základní rysy smlouvy 46

D.4 Vzorová smlouva: poznámky 46

Příloha E (informativní) Nakládání s velmi citlivými osobními zdravotními údaji 53

E.1 Úvod 53

E.2 Genetické nebo genomické údaje 53

E.3 Sociálně citlivé nebo infekční onemocnění 53

E.4 Informace o těhotenstvích a porodech 53

E.5 Zdravotní informace specifické dle kontextu 54

E.6 Kategorie „velmi citlivých“ osobních zdravotních údajů 54

E.7 Zajištění bezpečnosti „velmi citlivých“ osobních zdravotních údajů 54

Bibliografie 55



Veškerá práva vyhrazena. Pokud není specifikováno jinak, nesmí být žádná část této publikace reprodukována nebo používána v jakémkoliv formě nebo jakýmkoliv způsobem, elektronickým nebo mechanickým, včetně fotokopíí a mikrofilmů, bez písemného svolení buď od organizace ISO na níže uvedené adrese, nebo od členské organizace ISO v zemi žadatele.

ISO copyright office

Case postale 56 · CH-1211 Geneva 20

Tel. + 41 22 749 01 11

Fax + 41 22 749 09 47

E-mail copyright@iso.org

Web www.iso.org

Published in Switzerland

Předmluva

ISO (Mezinárodní organizace pro normalizaci) je celosvětová federace národních normalizačních orgánů (členů ISO). Mezinárodní normy obvykle vypracovávají technické komise ISO. Každý člen ISO, který se zajímá o předmět, pro který byla vytvořena technická komise, má právo být v této technické komisi zastoupen. Práce se zúčastňují také vládní i nevládní mezinárodní organizace, s nimiž ISO navázala pracovní styk. ISO úzce spolupracuje s Mezinárodní elektrotechnickou komisí (IEC) ve všech záležitostech normalizace v elektrotechnice.

Postupy použité při tvorbě tohoto dokumentu a postupy určené pro jeho další udržování jsou popsány ve směrnících ISO/IEC, část 1. Zejména se má věnovat pozornost rozdílným schvalovacím kritériím potřebným pro různé druhy dokumentů ISO. Tento dokument byl vypracován v souladu s redakčními pravidly uvedenými ve směrnících ISO/IEC, část 2. (viz www.iso.org/directives).

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO nelze činit odpovědnou za identifikaci jakéhokoliv nebo všech patentových práv. Podrobnosti o jakýchkoliv patentových právech identifikovaných během přípravy tohoto dokumentu budou uvedeny v úvodu a/nebo v seznamu patentových prohlášení obdržených ISO (viz www.iso.org/patents).

Jakýkoliv obchodní název použitý v tomto dokumentu se uvádí jako informace pro usnadnění práce uživatelů a neznamena schválení.

Vysvětlení významu specifických termínů a výrazů ISO, které se vztahují k posuzování shody, jakož i informace o tom, jak ISO dodržuje principy WTO týkající se technických překážek obchodu (TBT), jsou uvedeny na tomto odkazu URL: Foreword – Supplementary information

Za tento dokument je odpovědná komise ISO/TC 215 *Zdravotnická informatika*.

Toto druhé vydání nahrazuje první vydání (ISO 22857:2004), které bylo technicky revidováno.

Úvod

V souvislosti se zdravím je nutné shromažďovat, uchovávat a zpracovávat informace o jednotlivých osobách pro mnoho různých účelů, z nichž hlavními jsou

- přímé poskytování péče, například dokumentace pacientů;

- pojištění;
- klinický výzkum; a
- zdraví obyvatel.

Klasifikace účelů pro zpracování osobních zdravotních informací je uvedena v ISO/TS 14265.^[15]

Požadované údaje jsou závislé na účelu. V souvislosti s identifikací jednotlivců mohou být údaje nezbytné

- pro umožnění, aby byl jednatel rychle a jednoznačně identifikován (například kombinace jména, adresy, věku, pohlaví, identifikačního čísla);
- pro potvrzení, že dva soubory údajů patří ke stejnému jednateli bez jakékoli potřeby identifikovat jednotlivce samotného (například pro propojení záznamů a/nebo dlouhodobé statistiky); a
- pro jakékoliv účely, kde ale nejsou identifikovatelné údaje požadovány, by mělo být cílem zabránit takové identifikaci jednotlivce.

Za všech takových okolností jsou údaje o jednotlivcích nyní, a v budoucnu budou stále více předávány přes národní hranice/ hranice jurisdikce nebo budou záměrně zpřístupněny jiným státům/jurisdikcím, než ve kterých byly shromažďovány nebo uchovávány. Údaje mohou být shromažďovány v jednom státu/jurisdikci a uchovávány v jiném, upravovány v třetím a zpřístupněny z mnoho států/jurisdikcí nebo dokonce globálně. Základním požadavkem je to, že

- veškeré toto zpracovávání bude prováděno způsobem, který je v souladu s účely a obsahem původního souboru údajů a zejména,
- všechna zpřístupnění osobních zdravotních údajů by neměla přesahovat u příslušných jednotlivců nebo organizací rámec těchto účelů a obsahu.

Mezinárodní aplikace týkající se zdraví mohou vyžadovat, aby osobní zdravotní údaje byly předány z jednoho státu do druhého přes státní hranice. To je velice zřejmé v telemedicině nebo když jsou údaje zasílány elektronicky například emailem nebo souborem dat, který má být přidán do mezinárodní databáze. Může k tomu dojít také, ale méně zjevně, jestliže se nahlíží do databáze jednoho státu/jurisdikce z druhého státu například na internetu. Taková aplikace se může zdát pasivní, ale samotný akt nahlížení zahrnuje zpřístupnění údajů a považuje se za „zpracování“. Navíc vyžaduje stažení, které může být automaticky umístěno do mezipaměti a tam uchováno, dokud nebude „vymazána“ – to je také zpracování a znamená mimořádné nebezpečí. Stejně okolnosti mohou nastat, jestliže jsou údaje předány přes hranice jurisdikce.

Existuje široký okruh organizací, které by se mohly podílet na přijímání osobních zdravotních údajů z jiného státu/jurisdikce, například:

- zdravotnická zařízení jako jsou nemocnice;
- výzkumné databanky existující v jednom státu, ale zásobované s přístupem jiných států;
- dodavatelé, kteří dálkově spravují systémy zdravotní péče v jiných státech;
- organizace, které vedou vzdělávací databáze obsahující například radiologická zobrazení s diagnózami a záznamy k případu;
- společnosti, které vedou banky zdravotních záznamů pro pacienty z různých států/jurisdikcí;
- organizace, zabývající se mezinárodním nebo hranice jurisdikce překračujícím elektronickým obchodem, který se týká zdraví, jako je e-farmacie.

Ve všech aplikacích týkajících se osobních zdravotních údajů může existovat potenciální hrozba pro soukromí jednotlivce. Hrozba a její rozsah bude závislý na:

- úrovni, do jaké jsou údaje chráněny proti neautorizovanému přístupu při uchovávání nebo předávání;
- počtu osob, které mají autorizovaný přístup;
- povaze osobních zdravotních údajů;

- úrovni obtížnosti při identifikování jednotlivců, jestliže je získán přístup k údajům.

Kdykoliv jsou zdravotní údaje shromažďovány, uchovávány, zpracovávány nebo uveřejněny (včetně elektronicky na internetu), musí být posouzena potenciální hrozba ohledně soukromí a přijata příslušná ochranná opatření. Budou nezbytné nějaké formy analýzy rizik, aby se zjistila požadovaná úroveň bezpečnostních opatření.

Kromě normalizačních orgánů ISO, IEC, CEN a CENELEC existují čtyři hlavní mezinárodní orgány, které vytvořily mezinárodně závazné dokumenty týkající se bezpečnosti a ochrany údajů v kontextu přeshraničních toků:

- Organizace pro hospodářskou spolupráci a rozvoj (OECD);
- Rada Evropy;
- Spojené národy (UN);
- Evropská unie (EU).

Primární dokumenty těchto orgánů jsou:

- OECD „Směrnice o ochraně soukromí a přeshraničních toků osobních údajů“^[1];
- OECD „Směrnice o bezpečnosti informačních systémů“^[2];
- Rada Evropy „Úmluva o ochraně jednotlivců s ohledem na automatické zpracování osobních údajů“ č. 108^[3];
- „Doporučení Rady Evropy R(97)5 o ochraně zdravotních údajů“^[4];
- Valné shromáždění OSN „Pokyny pro regulování počítačově zpracovaných souborů osobních údajů“^[5];
- Směrnice EU o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.^[6]

Příloha A uvádí stručný přehled hlavních aspektů těchto dokumentů.

Prostředky a míra ochrany poskytovaná osobním zdravotním údajům se v jednotlivých zemích liší^[7] a v jednotlivých jurisdikcích. V některých státech jsou právní předpisy o ochraně soukromí s celostátní působností, v jiných mohou být právní předpisy na státní úrovni nebo ekvivalentu. V řadě států nemusí tyto právní předpisy existovat, ačkoliv mohou být zavedeny různé soubory postupů nebo ekvivalenty a/nebo mohou existovat „lékařské“ právní předpisy, které stanoví povinnost pro praktické lékaře, aby ochránily důvěrnost, integritu a dostupnost.

Ačkoliv právní předpisy o ochraně soukromí v různých částech světa mohou zmiňovat osobní zdravotní údaje, často neexistují zvláštní právní předpisy týkající se zdraví, možná s výjimkou ve vztahu k vládním agenturám a/nebo lékařskému výzkumu.

Příloha B obsahuje stručný nástin hlavních národních standardů nebo jiných dokumentovaných požadavků a právní stanovisko týkající se ochrany údajů v řadě států.

Osobní zdravotní údaje mohou být ve své podstatě mimořádně citlivé, a tudíž jsou k dispozici podrobné pokyny a normy jak na národní, tak i na mezinárodní úrovni týkající se různých administrativních a technických „bezpečnostních opatření“ pro ochranu osobních zdravotních údajů.

Tato mezinárodní norma se snaží využít a harmonizovat požadavky na ochranu údajů týkající se předávání osobních zdravotních údajů přes mezinárodní hranice, jak uvedeno v závazných mezinárodních dokumentech. Snaží se také vzít v úvahu řadu národních požadavků tak, aby se, je-li to možné, vyhnula rozporu mezi požadavky této mezinárodní normy a národními specifikacemi.

Nicméně tato mezinárodní norma se aplikuje výhradně na předávání osobních zdravotních údajů přes státní hranice/ hranice jurisdikce. Výslovně se nesnaží specifikovat národní nebo zvláštní požadavky jurisdikce na ochranu údajů. Vytvoření souboru opatření zaměřených na to, aby byly přijatelné pro

všechny státy/jurisdikce, ať vysílají nebo přijímají osobní zdravotní údaje do/z jiných zemí/jurisdikcí, nevyhnutelně znamená přijetí nejprísnějších požadavků. To znamená, že organizace v některých státech/jurisdikcích by měly aplikovat mimořádné nebo přísnější požadavky na ochranu údajů, když vysílají osobní zdravotní údaje do jiných států/jurisdikcí nebo je od jiných států/jurisdikcí přijmou, než by bylo nutné pro nakládání s takovými údaji v rámci jejich vlastních hranic. I když tomu tak může být, neznamená to, že takové mimořádné nebo přísnější požadavky musí být aplikovány na interní národní aplikace/aplikace v rámci jurisdikce.

Tato mezinárodní norma nespecifikuje, zda má být souhlas implicitní nebo explicitní nebo zda má nebo nemá být v písemné podobě nebo jejím ekvivalentu. Rovněž tak se nezabývá tím, jaká mají být přijata opatření, jestliže subjekt údajů není z jakéhokoliv důvodu schopen udělit smysluplný souhlas. Takové otázky mohou být specifikovány v právních předpisech státu/jurisdikce vývozce údajů nebo mohou být věcí zvyklosti nebo kultury v tomto státu/jurisdikci. Posuzování, které lze ideálně aplikovat na tyto aspekty, je takové, že souhlas je udělen v souladu s očekáváními, která by subjekt údajů měl při udělení tohoto souhlasu v souvislosti s jakýmikoliv jinými právními předpisy, zvyklostmi nebo kulturou, které se týkají subjektu údajů.

1 Předmět normy

Tato mezinárodní norma poskytuje pokyny k požadavkům na ochranu údajů za účelem usnadnění předání osobních zdravotních údajů přes národní hranice nebo hranice jurisdikce.

To nevyžaduje harmonizaci existujících národních předpisů, jurisdikčních norem, právních nebo správních předpisů. Je normativní pouze ve vztahu k mezinárodní výměně osobních zdravotních údajů nebo přes hranice jurisdikcí. Nicméně může být informativní s ohledem na ochranu zdravotních informací v rámci národních hranic/hranic jurisdikce a poskytovat pomoc národním nebo soudním orgánům, které jsou zapojeny do vývoje a implementace principů ochrany údajů.

Mezinárodní norma zahrnuje jak principy ochrany údajů, které se týkají mezinárodních přenosů nebo přenosů přes hranice jurisdikce, tak bezpečnostní politiku, kterou organizace přijme, aby zajistila soulad s těmito principy.

Jestliže byla mezi několika státy sjednána mnohostranná dohoda (například směrnice EU o ochraně údajů), budou mít podmínky této dohody přednost.

Cílem této mezinárodní smlouvy je napomáhat mezinárodním a přeshraničním jurisdikcím u zdravotních aplikací, které zahrnují předání osobních zdravotních údajů. Snaží se poskytnout prostředky, jejichž prostřednictvím zdravotní údaje, týkající se subjektů údajů, jako například pacientů, budou adekvátně chráněny při zasílání a zpracovávání v jiném státu/jurisdikci.

Tato mezinárodní norma neposkytuje konečné právní poradenství, ale obsahuje pokyny. Při použití pokynů na určitou aplikaci může být na tuto aplikaci využito řádné právní poradenství.

Národní požadavky na ochranu soukromí a údajů se podstatně liší a mohou se relativně rychle měnit. I když tato mezinárodní norma obecně zahrnuje přísnější mezinárodní a národní požadavky, obsahuje jich však jen minimum. Některé státy/jurisdikce mohou mít některé přísnější a specifické požadavky.

Konec náhledu - text dále pokračuje v placené verzi ČSN.