ČESKÁ TECHNICKÁ NORMA

ICS 35.240.80; 35.030

Listopad 2026

Zdravotnická informatika – Opatření informační bezpečnosti ve zdravotnictví založená na ISO/IEC 27002

ČSN
EN ISO 27799

98 2021

idt ISO 27799:2025

Health informatics – Information security controls in health based on ISO/IEC 27002

Informatique de santé – Contrôles de sécurité de l,information dans le domaine de la santé basés sur l,ISO/IEC 27002

Medizinische Informatik – Informationssicherheitsmanagement im Gesundheitswesen bei Verwendung der ISO/IEC 27002

Tato norma je českou verzí evropské normy EN ISO 27799:2026. Překlad byl zajištěn Českou agenturou pro stan-
dardizaci. Má stejný status jako oficiální verze.

This standard is the Czech version of the European Standard EN ISO 27799:2026. It was translated by the Czech Standardization Agency. It has the same status as the official version.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN EN ISO 27799 (98 2021) z června 2026.

Národní předmluva

Změny proti předchozí normě

Proti předchozí normě dochází ke změně způsobu převzetí EN ISO 27799:2026 do soustavy norem ČSN.
Zatímco ČSN EN ISO 27799 z června 2026 převzala EN ISO 27799:2026 schválením k přímému používání jako ČSN oznámením ve Věstníku ÚNMZ, tato norma ji přejímá překladem.

Norma je technickou revizí předchozího vydání. Text byl uveden do souladu s novou strukturou ISO/IEC 27002:2022 a jinými změnami této normy oproti předchozí verzi, byla doplněna opatření specifická pro zdravotnictví a doplněny informativní přílohy obsahující doplňkové pokyny ke kybernetické bezpečnosti ve zdravotnických organizacích.

Informace o citovaných dokumentech

ISO/IEC 27002:2022 zavedena v ČSN EN ISO/IEC 27002:2023 (36 9798) Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti

ISO 81001-1 dosud nezavedena

Souvisící ČSN

ČSN ISO 8601 (soubor) (97 8601) Datum a čas – Zobrazení pro výměnu informací

ČSN ISO/IEC 8859 (soubor) (36 9111) Informační technologie – Jedním 8-bitovým bytem kódované soubory grafických znaků

ČSN EN ISO/IEEE 11073 (soubor) (98 0014) Zdravotnická informatika – Interoperabilita zařízení

ČSN EN ISO 12052 (98 2001) Zdravotnická informatika – Digitální zobrazování a komunikace v medicíně (DICOM), včetně pracovního postupu a správy dat

ČSN EN ISO 13131 (98 0031) Zdravotnická informatika – Telemedicínské služby – Směrnice pro plánování kvality

ČSN EN ISO 13940:2016 (98 0006) Zdravotnická informatika – Systém pojmů pro zajištění kontinuity péče

ČSN P CEN ISO/TS 14265 (98 1038) Zdravotnická informatika – Kategorizace účelů zpracování osobních zdravotních informací

ČSN EN ISO 21298 (98 2017) Zdravotnická informatika – Funkční a strukturální role

ČSN EN ISO 22600 (soubor) (98 0023) Zdravotnická informatika – Privilegium vedení a řízení přístupu

ČSN ISO 22857 (98 2024) Zdravotnická informatika – Směrnice pro ochranu přeshraničních toků osobních zdravotních údajů

ČSN EN ISO 25237 (98 2020) Zdravotnická informatika – Pseudonymizace

ČSN EN ISO/IEC 27001:2023 (36 9797) Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Systémy managementu informační bezpečnosti – Požadavky

ČSN EN ISO/IEC 27005 (36 9790) Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí –
Pokyny pro management rizik informační bezpečnosti

ČSN EN ISO/IEC 27701 (36 9770) Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Systémy managementu informací o soukromí – Požadavky a návod

ČSN EN ISO 27789:2022 (98 2025) Zdravotnická informatika – Auditní záznamy elektronických zdravotních
záznamů

ČSN ISO/HL7 27931 (98 1027) Norma pro výměnu dat – Zdravotnictví úroveň sedm verze 2.5 – Aplikační protokol pro elektronickou výměnu dat v prostředí zdravotní péče

Vysvětlivky k textu této normy

V případě nedatovaných odkazů na evropské/mezinárodní normy jsou ČSN uvedené v článcích „Informace
o citovaných dokumentech“ a „Souvisící ČSN“ nejnovějšími vydáními, platnými v době schválení této normy. Při používání této normy je třeba vždy použít taková vydání ČSN, která přejímají nejnovější vydání nedatovaných evropských/mezinárodních norem (včetně všech změn).

Upozornění na národní poznámky

Do této normy byly do úvodu k článkům 0.1 a 0.3 a k článkům 3.1.1, 3.1.2 a 3.2 doplněny národní poznámky.

Vypracování normy

Zpracovatel odborného překladu: KORPAS Olomouc, IČO 73792781

Technická normalizační komise: TNK 20 Informační a komunikační technologie

Vydala: Česká agentura pro standardizaci, státní příspěvková organizace

Citované dokumenty a souvisící ČSN lze získat v e-shopu.

Česká agentura pro standardizaci je státní příspěvková organizace zřízená Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví na základě ustanovení § 5 odst. 2 zákona č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů.

EVROPSKÁ NORMA
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN ISO 27799

Leden 2026

ICS 35.240.80; 35.030

Nahrazuje
EN ISO 27799:2016

Zdravotnická informatika – Opatření informační bezpečnosti ve zdravotnictví založená na ISO/IEC 27002 (ISO 27799:2025)

Health informatics – Information security controls in health based on ISO/IEC 27002 (ISO 27799:2025)

Informatique de santé – Contrôles de sécurité de l,information dans le domaine de la santé basés sur l,ISO/IEC 27002 (ISO 27799:2025)

Medizinische Informatik – Informationssicherheitsmanagement im Gesundheitswesen bei Verwendung der ISO/IEC 27002 (ISO 27799:2025)

Tato evropská norma byla schválena CEN dne 2025-12-14.

Členové CEN jsou povinni splnit vnitřní předpisy CEN/CENELEC, v nichž jsou stanoveny podmínky, za kterých se této evropské normě bez jakýchkoliv modifikací uděluje status národní normy. Aktualizované seznamy a biblio-
grafické citace týkající se těchto národních norem lze obdržet na vyžádání v Řídicím centru CEN-CENELEC nebo u kteréhokoliv člena CEN.

Tato evropská norma existuje ve třech oficiálních verzích (anglické, francouzské, německé). Verze v každém jiném jazyce přeložená členem CEN do jeho vlastního jazyka, za kterou zodpovídá a kterou notifikuje Řídicímu centru CEN-CENELEC, má stejný status jako oficiální verze.

Členy CEN jsou národní normalizační orgány Belgie, Bulharska, České republiky, Dánska, Estonska, Finska, Francie, Chorvatska, Irska, Islandu, Itálie, Kypru, Litvy, Lotyšska, Lucemburska, Maďarska, Malty, Německa,
Nizozemska, Norska, Polska, Portugalska, Rakouska, Republiky Severní Makedonie, Rumunska, Řecka, Slovenska, Slovinska, Spojeného království, Srbska, Španělska, Švédska, Švýcarska a Turecka.

Evropský výbor pro normalizaci
European Committee for Standardization
Comité Européen de Normalisation
Europäisches Komitee für Normung
Řídicí centrum CEN-CENELEC: Rue de la Science 23, B-1040 Brusel
© 2026 CEN Veškerá práva pro využití v jakékoliv formě a jakýmikoliv prostředky
Ref. č. EN ISO 27799:2026 E
jsou celosvětově vyhrazena národním členům CEN.

Evropská předmluva

Tento dokument (EN ISO 27799:2026) vypracovala technická komise ISO/TC 215 *Zdravotnická informatika*
ve spolupráci s technickou komisí CEN/TC 251 *Zdravotnická informatika*, jejímž sekretariátem je NEN.

Této evropské normě je nutno nejpozději do července 2026 udělit status národní normy, a to buď vydáním identického textu, nebo schválením k přímému používání, a národní normy, které jsou s ní v rozporu, je nutno zrušit nejpozději do července 2026.

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. CEN nelze činit odpovědným za identifikaci jakéhokoliv nebo všech patentových práv.

Tento dokument nahrazuje EN ISO 27799:2016.

Jakákoli zpětná vazba a otázky týkající se tohoto dokumentu mají být adresovány národnímu normalizačnímu orgánu uživatele. Úplný seznam těchto orgánů lze nalézt na webových stránkách CEN.

Podle vnitřních předpisů CEN-CENELEC jsou tuto evropskou normu povinny zavést národní normalizační organizace následujících zemí: Belgie, Bulharska, České republiky, Dánska, Estonska, Finska, Francie, Chorvatska, Irska, Islandu, Itálie, Kypru, Litvy, Lotyšska, Lucemburska, Maďarska, Malty, Německa, Nizozemska, Norska, Polska, Portugalska, Rakouska, Republiky Severní Makedonie, Rumunska, Řecka, Slovenska, Slovinska, Spojeného království, Srbska, Španělska, Švédska, Švýcarska a Turecka.

Oznámení o schválení

Text ISO 27799:2025 byl schválen CEN jako EN ISO 27799:2026 bez jakýchkoliv modifikací.

Obsah

Strana

Předmluva..... 10

Úvod..... 11

1..... Předmět normy..... 13

2..... Citované dokumenty..... 13

3..... Termíny, definice a zkratky..... 13

3.1..... Termíny a definice..... 13

3.2..... Zkratky..... 14

4..... Obecně..... 15

4.1..... Struktura tohoto dokumentu..... 15

4.2..... Zabezpečení..... 15

4.3..... Výběr a uplatňování opatření..... 15

4.3.1... Určování opatření..... 15

4.3.2... Použití pokynů..... 16

4.3.3... Použití s ISO/IEC 27001:2022..... 16

5..... Organizační opatření..... 16

5.1..... Politiky pro informační bezpečnost..... 16

5.2..... Role a odpovědnosti v oblasti informační bezpečnosti..... 17

5.3..... Oddělení povinností..... 18

5.4..... Odpovědnosti managementu..... 18

5.5..... Kontakt s autoritami..... 18

5.6..... Kontakt se zvláštními zájmovými skupinami..... 18

5.7..... Zpravodajství o hrozbách..... 18

5.8..... Informační bezpečnost v řízení projektů..... 19

5.9..... Inventarizace informací a dalších souvisejících aktiv..... 19

5.10.... Přípustné používání informací a dalších souvisejících aktiv..... 19

5.11.... Vrácení aktiv..... 19

5.12.... Klasifikace informací..... 20

5.13.... Označování informací.....

..... 20

5.14.... Předávání
informací..... 21

5.15.... Řízení
přístupu..... 21

5.16.... Management
identit..... 22

5.17.... Autentizační
informace..... 22

5.18.... Přístupová
práva..... 22

5.19.... Informační bezpečnost ve vztazích
s dodavateli..... 23

5.20.... Řešení informační bezpečnosti v dohodách
s dodavateli..... 23

5.21.... Management informační bezpečnosti v dodavatelském řetězci
ICT..... 23

5.22.... Monitorování, přezkoumávání a management změn dodavatelských
služeb..... 23

5.23.... Informační bezpečnost při používání cloudových
služeb..... 24

5.24.... Plánování a příprava managementu incidentů informační
bezpečnosti..... 24

5.25.... Posuzování a rozhodování o událostech informační
bezpečnosti..... 24

5.26.... Odezva na incidenty informační
bezpečnosti..... 24

5.27.... Poučení se z incidentů informační
bezpečnosti..... 24

5.28.... Shromažďování
důkazů.....

..... 24

5.29.... Informační bezpečnost během narušení..... 24

5.30.... Připravenost ICT na zajištění kontinuity činnosti organizace..... 24

5.31.... Zákonné, statutární, regulatorní a smluvní požadavky..... 25

5.32.... Práva duševního vlastnictví..... 25

5.33.... Ochrana záznamů..... 25

5.34.... Soukromí a ochrana PII..... 25

5.35.... Nezávislé přezkoumávání informační bezpečnosti..... 26

5.36.... Dodržování politik, pravidel a norem pro informační bezpečnost..... 26

5.37.... Dokumentované provozní postupy..... 26

5.38.... HLT – Analýza a specifikace požadavků na informační bezpečnost..... 27

5.39.... HLT – Jednoznačná identifikace subjektů péče..... 28

5.40.... HLT – Validace zobrazených/vytištěných dat..... 28

5.41.... HLT – Veřejně dostupné zdravotnické informace..... 29

5.42.... HLT – Nouzová komunikace..... 30

5.43.... HLT – Hlášení vnějších incidentů..... 30

6..... Opatření v oblasti lidských

zdrojů..... 31

6.1.....
Prověřování.....
..... 31

6.2..... Podmínky pracovního
poměru.....
31

6.3..... Povědomí, vzdělávání a školení o informační
bezpečnosti..... 31

6.4..... Disciplinární
řízení.....
..... 31

6.5..... Odpovědnosti po ukončení nebo změně pracovního
poměru..... 32

6.6..... Dohody o důvěrnosti nebo
mlčenlivosti..... 32

6.7..... Práce na
dálku.....
..... 32

6.8..... Podávání zpráv o událostech informační
bezpečnosti..... 32

6.9..... HLT – Školení
managementu.....
..... 33

7..... Opatření fyzické
bezpečnosti.....
..... 33

7.1..... Perimetry fyzické
bezpečnosti.....
..... 33

7.2..... Fyzický
vstup.....
..... 33

7.3..... Zabezpečení kanceláří, místností
a vybavení..... 34

7.4..... Monitorování fyzické
bezpečnosti.....
34

7.5..... Ochrana před fyzickými a přírodními hrozbami..... 34

7.6..... Práce v zabezpečených oblastech..... 34

7.7..... Prázdný stůl a prázdná obrazovka..... 34

7.8..... Umístění a ochrana zařízení..... 34

7.9..... Bezpečnost aktiv mimo prostory organizace..... 34

7.10.... Paměťová média..... 34

7.11.... Podpůrné služby..... 35

7.12.... Bezpečnost kabelových rozvodů..... 35

7.13.... Údržba zařízení..... 36

7.14.... Bezpečná likvidace nebo opakované použití zařízení..... 36

8..... Technologická opatření..... 36

8.1..... Koncová zařízení uživatele..... 36

8.2..... Privilegovaná přístupová práva..... 36

8.3..... Omezení přístupu k informacím..... 36

8.4..... Přístup ke zdrojovému kódu..... 36

8.5..... Bezpečná autentizace..... 36

8.6..... Management kapacit..... 37

8.7..... Ochrana před škodlivým softwarem..... 37

8.8..... Management technických zranitelností..... 37

8.9..... Management konfigurací..... 37

8.10.... Vymazání informací..... 38

8.11.... Maskování dat..... 38

8.12.... Prevence úniku dat..... 38

8.13.... Zálohování informací..... 38

8.14.... Redundance vybavení pro zpracování informací..... 39

8.15.... Zaznamenávání formou logů..... 39

8.16.... Monitorovací činnosti..... 39

8.17.... Synchronizace hodin..... 39

8.18.... Používání privilegovaných obslužných programů..... 39

8.19.... Instalace softwaru na provozních systémech..... 39

8.20.... Bezpečnost sítí..... 39

8.21.... Bezpečnost síťových služeb..... 39

8.22.... Oddělení sítí..... 39

8.23.... Filtrování webových stránek..... 40

8.24.... Používání kryptografie..... 40

8.25.... Životní cyklus bezpečného vývoje..... 40

8.26.... Požadavky na bezpečnost aplikací..... 40

8.27.... Principy architektury a inženýrství bezpečných systémů..... 40

8.28.... Bezpečné programování..... 40

8.29.... Testování bezpečnosti při vývoji a akceptaci..... 40

8.30.... Vývoj zajišťovaný externími zdroji..... 40

8.31.... Oddělení prostředí vývoje, testování a produkce..... 40

8.32.... Management změn..... 41

8.33.... Informace pro testování..... 41

8.34.... Ochrana informačních systémů během auditního testování..... 41

8.35.... HLT – Principy nulové důvěry..... 41

Příloha A (informativní) Opatření informační bezpečnosti v oblasti zdravotní péče..... 42

Příloha B (informativní) Soulad tohoto dokumentu s ISO 27799:2016..... 44

Příloha C (informativní) Informační bezpečnost ve zdravotnických organizacích..... 45

Příloha D (informativní) Příklady požadavků na bezpečnost a soukromí ve zdravotnických informačních systémech a jejich mapování na opatření podle ISO 27799 a bezpečnostní funkce podle IEC/TS 81001-2-2..... 54

Bibliografie..... 74

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 směrnicích 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 směrnicích ISO/IEC, část 2 (viz www.iso.org/directives).

ISO upozorňuje na možnost, že implementace tohoto dokumentu může vyžadovat využití patentu (patentů). V souvislosti s tím ISO nezaujímá žádné stanovisko týkající se důkazů, platnosti nebo použitelnost všech uplatňovaných patentových práv. Ke dni zveřejnění tohoto dokumentu ISO neobdržela oznámení o patentu (patentech), který smí být vyžadován pro implementaci tohoto dokumentu. ISO však upozorňuje implementující organizace, že se nemusí jednat o nejnovější informace, které lze získat z databáze patentů dostupné na adrese www.iso.org/patents. ISO nelze činit odpovědnou za identifikaci jakéhokoliv nebo všech takových patentových práv.

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

Vysvětlení nezávazného charakteru technických norem, významu specifických termínů a výrazů ISO, které se vztahují k posuzování shody, jakož i informace o tom, jak ISO dodržuje principy Světové obchodní organizace (WTO) týkající se technických překážek obchodu (TBT), viz www.iso.org/iso/foreword.html.

Tento dokument vypracovala technická komise ISO/TC 215 *Zdravotnická informatika*, ve spolupráci s technickou komisí Evropského výboru pro normalizaci (CEN) CEN/TC 251 *Zdravotnická informatika* na základě Dohody o technické spolupráci mezi ISO a CEN (Vídeňská dohoda).

Toto třetí vydání zrušuje a nahrazuje ISO 27799:2016 a ISO/TS 14441:2013, které byly technicky zrevidovány.

Hlavní změny jsou:

- uvedení do souladu s novou strukturou ISO/IEC 27002:2022 a jinými změnami této normy oproti předchozí verzi;
- revize a doplnění opatření specifických pro zdravotnictví;
- vypuštění materiálu, které byl původně pouze ve druhém vydání tohoto dokumentu, ale následně byl začleněn do ISO/IEC 27002:2022;
- doplnění informativních příloh obsahujících doplňkové pokyny ke kybernetické bezpečnosti ve zdravotnických organizacích a na základě ISO/TS 14441:2013, 5.3 aktualizovaných příkladů požadavků na bezpečnost a soukromí ve zdravotnických informačních systémech.

Jakákoli zpětná vazba nebo otázky týkající se tohoto dokumentu mají být adresovány národnímu

normalizačnímu orgánu uživatele. Úplný seznam těchto orgánů lze nalézt na adrese www.iso.org/members.html.

Úvod

0.1 Obecně

Tento dokument obsahuje soubor opatření informační bezpečnosti ve zdravotnických organizacích. Zahrnuje všechna opatření uvedená v ISO/IEC 27002:2022 a v některých případech tato opatření doplňuje nebo uvádí pokyny k jejich použití ve zdravotnictví[NP1)]. Uvedena jsou zde také některá dodatečná opatření specifická pro zdravotnictví, která nejsou odvozena z žádných opatření v ISO/IEC 27002:2022.

0.2 Kontext a pozadí

K faktorům ovlivňujícím informační bezpečnost ve zdravotní péči patří tyto:

a) Používání vybavení, jehož provoz závisí na digitálních technologiích a které je používáno výlučně nebo převážně ve sféře zdravotní péče. Typickým příkladem jsou zdravotnické prostředky s integrovaným zdravotnickým softwarem.

b) Potřeba nalezení rovnováhy mezi klinickou bezpečností a efektivitou a informační bezpečností.

c) Zachování soukromí subjektů péče při zajišťování přístupu k příslušným osobním zdravotním informacím pro stanovení diagnózy a léčbu.

d) Distribuovaná povaha osobních zdravotních informací v rámci organizace i mezi organizacemi (případně v různých jurisdikcích), jejímž důsledkem je nezbytnost vysoké úrovně interoperability mezi různými systémy, aplikacemi a prostředky.

e) Různé typy uživatelů včetně lékařů, zdravotních sester, jiných klinických pracovníků, stážistů, studentů, asistentů ve zdravotní péči, techniků, administrativních pracovníků a dobrovolníků, stejně jako subjektů péče a jejich zástupců.

f) Mnohé vzájemné závislosti a toky informací v rámci organizace i mezi organizacemi zabývajícími se zdravotní péčí, klinickým výzkumem, výukou, vzděláváním a školením nebo více z těchto činností.

g) Potřeba nepřetržité (24 hodin denně) dostupnosti některých služeb zdravotní péče za normálních okolností. Navíc přírodní katastrofy a jiné neobvyklé události, které mohou vést k prudkému nárůstu potřeby služeb zdravotní péče.

h) Organizace poskytující zdravotní služby, stejně jako výrobci nebo dodavatelé systémů, zařízení a vybavení podléhají široké škále právních, zákonných, správních a smluvních ustanovení, která se mohou v jednotlivých jurisdikcích lišit.

i) Překrývající se nebo neúplné požadavky na zodpovědnost a profesní odpovědnost mezi různými profesemi (např. ICT pracovníci a pracovníci obsluhující zdravotnické prostředky) pro zajištění zabezpečení a bezpečnosti systémů, zařízení a vybavení.

S přihlédnutím k tomuto všeobecnému kontextu má odvětví zdravotní péče řadu požadavků na informační bezpečnost, které jsou specifické, a někdy dokonce jedinečné. Opatření v ISO/IEC 27002:2022 jsou však záměrně obecná, proto je zapotřebí tento dokument.

0.3 Cílová skupina a využití

Tento dokument je určen organizacím, které:

- poskytují zdravotní služby[NP2)] nebo jsou správci osobních zdravotních informací z jiných důvodů;
- dodávají software, systémy, zařízení, vybavení nebo služby, které se používají pro zpracování osobních zdravotních informací;
- jsou zodpovědné za předpisy, akreditace, prohlídky, zajištění apod. ve zdravotní péči.

K jednotlivcům, kterým je tento dokument určen zejména, patří:

- odborníci obsluhující ICT nebo odborníci obsluhující zdravotnické prostředky nebo přístroje, pracující v typech organizací uvedených výše;

- odborníci na informační bezpečnost (zvláště ti, kteří nejsou obeznámeni se sférou zdravotnictví): mezi tyto odborníky se mohou řadit konzultanti, penetrační testeři, auditoři a zaměstnanci orgánů zajišťujících akreditační, inspekční, záruční nebo certifikační služby informační bezpečnosti.

Vhodná implementace opatření v tomto dokumentu může poskytovat ujištění jednotlivcům, včetně subjektů péče, jejich zástupcům a zaměstnancům organizace. Vhodná implementace může také poskytovat záruky celé řadě zúčastněných stran včetně managementu a dozorčích rad zdravotnických organizací, jiných zdravotnických
organizací, s nimiž vyměňují nebo sdílí informace, veřejných orgánů, regulačních orgánů, auditorů a organizací, které financují, pojišťují, akreditují nebo dozorují služby zdravotní péče.

Tento dokument může ve zdravotnických zařízeních sloužit při určování a implementaci opatření systémů
managementu informační bezpečnosti (ISMS) v souladu s ISO/IEC 27001.

1 Předmět normy

Tento dokument obsahuje opatření informační bezpečnosti, včetně pokynů k implementaci, pro zdravotnické organizace. Je založen na ISO/IEC 27002:2022.

Vedle obecných ICT zařízení a softwaru používaných v mnoha jiných prostředích zahrnuje rozsah platnosti tohoto dokumentu software a systémy specifické pro zdravotní péči, jako jsou systémy elektronických zdravotních
záznamů a zdravotnické prostředky s integrovaným zdravotnickým softwarem. Takové zdravotnické prostředky mohou být naprogramované nebo programovatelné a mohou obsahovat software, firmware nebo obojí.

Do rozsahu platnosti tohoto dokumentu spadají rovněž jiná digitální zařízení (např. pro environmentální a infekční opatření, správu budov a fyzickou bezpečnost), která mohou být používána v prostorách pro poskytování zdravotní péče.

Tento dokument se vztahuje na informace v různých pohledech a podobách (včetně textu a čísel, zvukových
záznamů, nákresů, zobrazení a videí), pořízené a zaznamenané libovolnými prostředky, k jejich uložení se použí-
vají libovolné prostředky (jako je tisk nebo písmo nebo elektronické uložení) a pro jejich přenos nebo výměnu slouží libovolné prostředky (přenos ústně, písemně, poštou, přenosem paměťových médií, přímými odkazy nebo prostřednictvím sítě).

Tento dokument je určen organizacím všech typů a velikostí, které poskytují zdravotní péči nebo jsou správci osobních zdravotních informací z jiných důvodů. Informace, za něž nesou odpovědnost, mohou být ukládány a zpracovávány mnoha různými způsoby a na mnoha místech, včetně fyzického prostoru nebo cloudových služeb, nadále však spadají do rozsahu platnosti tohoto dokumentu.

Tento dokument platí pro všechna fyzická prostředí, která mají sloužit k poskytování zdravotní péče, jako jsou nemocnice, kliniky a jiná místa, nebo zařízení využívaná pro účely zdravotní péče, jako jsou ambulance a mobilní zobrazovací nebo diagnostické jednotky. Platí také pro péči poskytovanou jinde, např. v obytných prostorách. Vedle nejrůznějších prostředí tento dokument platí i pro všechny způsoby poskytování služeb včetně zdravotní péče na dálku nebo virtuální zdravotní péče.

Konec náhledu - text dále pokračuje v placené verzi ČSN.

NP1) NÁRODNÍ POZNÁMKA Termín „zdravotnictví“ byl zde i v názvu normy zvolen s ohledem na jeho dřívější zavedení
ve zdrojové normě a dalších souvisejících normách. Přesnější by byl spíše překlad „zdraví“, protože norma se vztahuje na organizace všech typů, které poskytují zdravotní péči nebo jsou z jiných důvodů depozitáři osobních zdravotních informací. Tedy i např. na poskytovatele sociálně-zdravotních služeb nebo ošetřovatelské péče, pojišťovny, výzkumné instituce, výrobce aplikací, zaměstnavatele atp.

NP2) NÁRODNÍ POZNÁMKA Zdravotní služby a podmínky jejich poskytování upravuje česká legislativa v Zákoně č. 372/2011 Sb. (Zákon o zdravotních službách). Požadavky uvedené v této normě se týkají všech druhů a forem zdravotních služeb v tomto zákoně uvedených.