ČESKÁ TECHNICKÁ NORMA

ICS 35.240.80 **Únor**
2019

Zdravotnická informatika – Systémy řízení bezpečnosti informací ve zdravotnictví využívající ISO/IEC 27002

ČSN
EN ISO 27799

98 2021

idt ISO 27799:2016

Health informatics – Information security management in health using ISO/IEC 27002

Informatique de santé – Management de la sécurité de l,information relative a la santé en utilisant l,ISO/IEC 27002

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

Tato norma je českou verzí evropské normy EN ISO 27799:2016. Překlad byl zajištěn Českou agenturou pro standardizaci. Má stejný status jako oficiální verze.

This standard is the Czech version of the European Standard EN ISO 27799:2016. It was translated by the Czech Agency for Standardization. It has the same status as the official version.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN EN ISO 27799 (98 2021) z února 2017.

Národní předmluva

Změny proti předchozí normě

Proti předchozí normě dochází ke změně způsobu převzetí EN ISO 27799:2016 do soustavy norem ČSN. Zatímco ČSN EN ISO 27799 (98 2021) z února 2017 převzala EN ISO 27799:2016 schválením k přímému používání jako ČSN oznámením ve Věstníku ÚNMZ, tato norma ji přejímá překladem.

Informace o citovaných dokumentech

ISO/IEC 27000 zavedena v ČSN EN ISO/IEC 27000 (36 9790) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník

ISO/IEC 27002 zavedena v ČSN EN ISO/IEC 27002 (36 9798) Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací

Souvisící ČSN

ČSN P CEN ISO/TS 14441:2014 (98 2026) Zdravotnická informatika – Požadavky na bezpečnost a důvěrnost systémů EHR při ověřování shody

ČSN ISO 15489-1 (97 1500) Informace a dokumentace – Správa dokumentů – Část 1: Pojmy a principy

TNI ISO/TR 17791:2015 (98 0025) Zdravotnická informatika – Pokyn k normám pro zabezpečení zdravotnického softwaru

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

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

ČSN EN ISO 22301 (01 2306) Ochrana společnosti – Systémy managementu kontinuity podnikání – Požadavky

ČSN EN ISO 22313 (01 2316) Ochrana společnosti – Systémy managementu kontinuity podnikání – Pokyny

ČSN EN ISO 22600-1 (98 0023) Zdravotnická informatika – Privilegium vedení a řízení přístupu – Část 1: Přehled a politika

ČSN EN ISO 22600-2 (98 0023) Zdravotnická informatika – Privilegium vedení a řízení přístupu – Část 2: Formální modely

ČSN EN ISO 22600-3 (98 0023) Zdravotnická informatika – Privilegium vedení a řízení přístupu – Část 3: Implementace

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

ČSN EN ISO/IEC 27001:2014 (36 9797) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky

ČSN ISO/IEC 27005 (36 9790) Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti
informací

ČSN ISO/IEC 27007 (36 9790) Informační technologie – Bezpečnostní techniky – Směrnice pro audit systémů řízení

ČSN ISO/IEC 27031 (36 9801) Informační technologie – Bezpečnostní techniky – Směrnice pro připravenost informačních a komunikačních technologií pro kontinuitu činnosti organizace

ČSN ISO/IEC 27033-1 (36 9701) Informační technologie – Bezpečnostní techniky – Bezpečnost sítě – Část 1: Přehled a pojmy

ČSN ISO/IEC 27033-2 (36 9701) Informační technologie – Bezpečnostní techniky – Bezpečnost sítě – Část 2: Směrnice pro návrh a implementaci bezpečnosti sítě

ČSN ISO/IEC 27033-3 (36 9701) Informační technologie – Bezpečnostní techniky – Bezpečnost sítě – Část 3: Referenční síťové scénáře – Hrozby, techniky návrhu a otázky řízení

ČSN ISO/IEC 27033-4 (36 9701) Informační technologie – Bezpečnostní techniky – Bezpečnost sítě –

Část 4: Zabezpečení komunikace mezi sítěmi s využitím bezpečnostních bran

ČSN ISO/IEC 27033-5 (36 9701) Informační technologie – Bezpečnostní techniky – Bezpečnost sítě – Část 5: Zabezpečení komunikace napříč sítěmi použitím virtuálních privátních sítí (VPN)

ČSN EN ISO/IEC 27037 (36 9846) Informační technologie – Bezpečnostní techniky – Směrnice pro identifikaci, sběr, získávání a uchovávání digitálních důkazů

ČSN EN ISO 27789:2013 (98 2025) Zdravotnická informatika – Auditní záznamy elektronických zdravotních
záznamů

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

ČSN ISO/IEC 29100 (36 9705) Informační technologie – Bezpečnostní techniky – Rámec soukromí

ČSN ISO/IEC 29101 (36 9708) Informační technologie – Bezpečnostní techniky – Rámec architektury soukromí

ČSN ISO 31000 (01 0351) Management rizik – Principy a směrnice

Vysvětlivky k textu převzaté normy

V souladu s ČSN ISO/IEC 27002:2014 byl pro účely této normy použit překlad anglického termínu „control“ jako „opatření“, „řízení“ nebo „kontrola“ s ohledem na význam v textu normy.

Pro účely této normy byl použit překlad anglického termínu „guidance“ jako „pokyny“ vzhledem k jeho používání v oblasti IT a v souladu s vydanými normami z oblasti IT, zejména normami řady ISO/IEC 27XXX a řady ISO/IEC 29XXX. Český ekvivalent „návod“ je vzhledem ke kontextu nevhodný a v praxi se v souvislosti s uvedenými řadami norem nepoužívá.

Pro účely této normy byly použity následující anglické termíny v původní podobě, vzhledem k rozšíření těchto termínů v odborné komunitě a/nebo absenci českého ekvivalentu:

malware, benchmarking

Upozornění na národní poznámky

Do kapitoly B.4 byly doplněny národní poznámky upozorňující na nesprávné číslování článků v této kapitole.

Vypracování normy

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

Technická normalizační komise: TNK 20 Informační technologie

Pracovník České agentury pro standardizaci: Ing. Miroslav Škop

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 EN ISO 27799
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM Srpen 2016

ICS 35.240.80 Nahrazuje
EN ISO 27799:2008

Zdravotnická informatika – Systémy řízení bezpečnosti informací ve zdravotnictví využívající ISO/IEC 27002
(ISO 27799:2016)

Health informatics – Information security management in health using ISO/IEC 27002
(ISO 27799:2016)

Informatique de santé – Management de la sécurité
de l,information relative a la santé en utilisant l,ISO/IEC 27002
(ISO 27799:2016)

Medizinische Informatik – Informationsmanagement
im Gesundheitswesen bei Verwendung der ISO/IEC 27002
(ISO 27799:2016)

Tato evropská norma byla schválena CEN dne 2016-06-18.

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 Řídicím centru CEN-CENELEC, má stejný status jako oficiální verze.

Evropský výbor pro normalizaci
European Committee for Standardization
Comité Européen de Normalisation
Europäisches Komitee für Normung
Řídicí centrum CEN-CENELEC: Avenue Marnix 17, B-1000 Brusel
© 2016 CEN Veškerá práva pro využití v jakékoli formě a jakýmikoli prostředky
Ref. č. EN ISO 27799:2016 E
jsou celosvětově vyhrazena národním členům CEN.

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

Evropská předmluva

Tento dokument (EN ISO 27799:2016) vypracovala technická komise ISO/TC 215 *Zdravotnická informatika* ve spolupráci s technickou komisí CEN/TC 251 *Zdravotnická informatika*, jejíž sekretariát zajišťuje NEN.

Této evropské normě je nutno nejpozději do února 2017 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 února 2017.

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

Tento dokument nahrazuje EN ISO 27799:2008.

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

Oznámení o schválení

Text ISO 27799:2016 byl schválen CEN jako EN ISO 27799:2016 bez jakýchkoliv modifikací.

Obsah

Strana

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).

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 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 neznamená 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 zrušuje a nahrazuje první vydání (ISO 27799:2008), které bylo technicky zrevidováno.

Úvod

Tato norma poskytuje pokyny zdravotnickým organizacím a jiným správcům osobních zdravotních informací, jak nejlépe ochránit důvěrnost, integritu a dostupnost takových informací. Je založená na a rozšiřuje obecné pokyny stanovené v ISO/IEC 27002:2013 a zaměřuje se na specifické potřeby řízení bezpečnosti informací v resortu zdravotnictví a v jeho specifických provozních podmínkách. Ačkoliv ochrana a bezpečnost osobních zdravotních informací je důležitá pro všechny jednotlivce, organizace, instituce a vlády, sektor zdravotnictví má zvláštní požadavky, které musí být splněny, aby byla zajištěna důvěrnost, integrita, auditovatelnost a dostupnost osobních zdravotních informací. Tento druh informací je považován za nejdůvěrnější ze všech druhů osobních informací. Ochrana této důvěrnosti je nezbytná, pokud má být zajištěno soukromí subjektů péče. Integrita zdravotnických informací musí být chráněna, aby bylo zajištěno bezpečí pacientů, a důležitou součástí této ochrany je zajištění auditovatelnosti celého životního cyklu informací. Dostupnost zdravotnických informací je také rozhodující z hlediska efektivity výkonu zdravotní péče. Zdravotnické informační systémy musí splňovat zvláštní požadavky, aby byly akceschopné při přírodních katastrofách, selháních systému a při útocích typu odmítnutí služby. Ochrana důvěrnosti, integrity a dostupnosti zdravotnických informací proto vyžaduje odbornou způsobilost v resortu zdravotnictví.

Bez ohledu na velikost, umístění a formu poskytování služeb všechny zdravotnické organizace musí mít zavedena nezbytná přísná opatření, aby chránila jim svěřené zdravotnické informace. Stále ještě mnoho odborných pracovníků ve zdravotnictví pracuje jako samostatný poskytovatel zdravotních služeb nebo v malých klinikách, kterým chybí specializované IT zdroje na řízení bezpečnosti informací. Zdravotnické organizace proto musí mít jasné, stručné a zdravotně-specifické pokyny týkající se výběru a provozování těchto opatření. Tato norma musí být přizpůsobitelná široké škále poskytovatelů služeb ve zdravotnictví dle rozsahu, umístění nebo formy. Konečně v souvislosti s elektronickou výměnou osobních zdravotních informací mezi odbornými pracovníky ve zdravotnictví (včetně použití bezdrátových a internetových služeb), existuje jasný přínos v přijetí společných doporučení pro řízení bezpečnosti informací ve zdravotnictví.

ISO/IEC 27002 je již široce používána pro zdravotnickou informatiku řízení bezpečnosti IT prostřednictvím působení národních nebo regionálních směrnic v Austrálii, Kanadě, Francii, Nizozemí, Novém Zélandu, Jižní Africe a ve Velké Británii a jinde. ISO 27799 staví na zkušenostech získaných v rámci těchto národních snah při řešení bezpečnosti osobních zdravotních informací a je určena jako doprovodný dokument k ISO/IEC 27002. Není určena k nahrazení norem řady ISO/IEC 27000. Spíše se jedná o doplnění těchto více obecných norem.

ISO 27799 aplikuje ISO/IEC 27002 do oblasti zdravotnictví způsobem, který pečlivě zvažuje vhodné uplatnění bezpečnostních kontrol za účelem ochrany osobních zdravotních informací. V některých případech vedly tyto úvahy autory k závěru, že použití určitých kontrolních cílů ISO/IEC 27002 je nezbytné, pokud mají být osobní zdravotní informace odpovídajícím způsobem chráněny. ISO 27799 proto omezuje aplikaci některých bezpečnostních kontrol definovaných v ISO/IEC 27002.

Všechny cíle bezpečnostních opatření popsané v ISO/IEC 27002 jsou důležité pro zdravotnickou informatiku, ale některá opatření vyžadují další vysvětlení, jak mohou být nejlépe použita k ochraně důvěrnosti, integrity a dostupnosti zdravotních informací. Existují také další specifické požadavky pro sektor zdravotnictví. Tato norma poskytuje další pokyny ve formátu, který osoby odpovědné za bezpečnost zdravotních informací snadno pochopí a přijmou.

V oblasti zdravotnictví je možné, aby organizace (řekněme nemocnice) byla certifikována tím, že používá ISO/IEC 27001 bez požadavku certifikace dle nebo i přijetí ISO 27799. Je třeba doufat že, jak se zdravotnické organizace snaží zlepšit bezpečnost osobních zdravotních informací, tak se

rozšíří soulad s ISO 27799 jako přísnější normy pro poskytování zdravotní péče.

Cíle

Zachování důvěrnosti, dostupnosti a integrity informací (včetně autenticity, odpovědnosti a auditovatelnosti) je zastřešujícím cílem bezpečnosti informací. V oblasti zdravotní péče závisí soukromí subjektů péče na zachování důvěrnosti osobních zdravotních informací. K zachování důvěrnosti musí být také přijata opatření k zachování integrity dat přinejmenším z důvodu, že je možné poškodit integritu dat řízení přístupu, auditních záznamů a jiných systémových dat způsobem, který umožní, aby došlo k narušení důvěrnosti nebo že tato narušení zůstanou bez povšimnutí. Kromě toho je na zachování integrity osobních zdravotních informací závislá bezpečnost pacienta, nesplnění tohoto požadavku, může také mít za následek onemocnění, zranění nebo dokonce i úmrtí. Rovněž vysoká úroveň dostupnosti je zvláště důležitým atributem zdravotnických systémů, kde je ošetření často náročné na včasnost. Zajisté přírodní katastrofy, které mohou vést k výpadkům jiných, nikoliv zdravotnických, IT systémů, mohou být právě tím okamžikem, kdy informace obsažené ve zdravotnických systémech jsou co nejvíce zapotřebí. Kromě toho útoky na systémy sítí typu odmítnutí služby jsou stále častější.

Opatření popisovaná v této normě jsou identifikována jako vhodná pro zdravotní péči při ochraně důvěrnosti, integrity a dostupnosti osobních zdravotních informací a k zajištění, že přístup k těmto informacím může být auditován a zdůvodněn. Tato opatření napomáhají zabránit chybám v lékařské praxi, které by mohly být důsledkem selhání v zajištění integrity zdravotnických informací. Kromě toho pomáhají zachovat kontinuitu lékařských služeb.

Existují ještě další aspekty, které formují cíle bezpečnosti zdravotnických informací. Zahrnují následující:

a) dodržování legislativních závazků uvedených v platných zákonech a předpisech zajišťujících ochranu práva subjektů péče na soukromí;1)

b) zachování stanovených osvědčených postupů na soukromí a bezpečnost ve zdravotnické informatice;

c) udržování individuální a organizační odpovědnosti mezi zdravotnickými organizacemi a odbornými pracovníky ve zdravotnictví;

d) podpora implementace systematického řízení rizik v rámci zdravotnických organizací;

e) plnění bezpečnostních potřeb zjištěných v běžné zdravotnické praxi;

f) snižování provozních nákladů usnadněním většího využívání technologií bezpečným, zabezpečeným a dobře řízením způsobem, který podporuje, ale neomezuje stávající zdravotnické aktivity;

g) udržování důvěry veřejnosti ve zdravotnické organizace a informační systémy, na které tyto organizace spoléhají;

h) udržování profesionálních standardů a etických zásad stanovených profesními lékařskými organizacemi (vzhledem k tomu, že bezpečnost informací zachovává důvěrnost a integritu zdravotnických informací);

i) provozování elektronických zdravotnických informačních systémů v prostředí vhodně zabezpečeném proti hrozbám;

j) usnadnění interoperability mezi zdravotnickými systémy, protože zdravotnické informace rostoucí měrou obíhají mezi zdravotnickými organizacemi a přes hranice soudní působnosti (zvláště když taková interoperabilita zdokonaluje správné zacházení se zdravotními informacemi k zajištění jejich stálé důvěrnosti, integrity a dostupnosti).

Vztah k řízení informací2), řízení organizace a klinické řízení

Zatímco postoje zdravotnických organizací ke klinickému řízení a řízení organizace se mohou lišit, důležitost začleňování a věnování pozornosti řízení informací, jako životně důležité opory obou, by měla být mimo veškerou diskusi. Čím více se zdravotnické organizace stávají kriticky závislé na informačních systémech na podporu péče (například využití technologií pro podporu rozhodování a vývoje směrem ke zdravotnické péči založené spíše na „důkazech“ než na „zkušenostech“), tím je více zřejmé, že události vedoucí ke ztrátě integrity, dostupnosti a důvěrnosti mohou mít velký klinický dopad, a na problémy vyplývající z těchto dopadů bude pohlíženo jako na selhání etických a zákonných povinností plynoucích z „povinné péče“.

Všechny země a jurisdikce budou nepochybně mít případové studie, kdy tato porušení vedla k chybným diagnózám, úmrtím nebo ke zdlouhavé rekonvalescenci. Pro systém klinického řízení je proto efektivní řízení rizik bezpečnosti informací stejně důležité jako plány léčebné péče, strategie pro řízení infekčních onemocnění a jiné „klíčové“ záležitosti klinického řízení. Tato norma bude nápomocna těm, kteří jsou zodpovědní za klinické řízení, aby pochopili přínos vytvořený účinnými strategiemi bezpečnosti informací.

Zdravotnické informace, které mají být chráněny

Existuje několik typů informací, jejichž důvěrnost, integritu a dostupnost3) je třeba chránit:

a) osobní zdravotní informace,

b) pseudonymizovaná data získaná z osobní zdravotní informace prostřednictvím některé metodiky pro pseudonymní identifikaci,

c) statistické a výzkumné údaje, včetně anonymizovaných dat, získaných z osobní zdravotní informace odstraněním osobních identifikačních údajů,

d) lékařské znalosti, které nesouvisí se žádným konkrétním subjektem péče, včetně klinických dat na podporu rozhodování (například údaje o nežádoucích účincích léků),

e) údaje o odborných pracovnicích ve zdravotnictví, zaměstnancích a dobrovolnících,

f) informace týkající se veřejného dohledu nad zdravotnictvím,

g) data auditních záznamů vytvářená zdravotnickými informačními systémy, které obsahují osobní zdravotní informace nebo pseudonymizovaná data získaná z osobních zdravotních informací nebo obsahují údaje o činnostech uživatelů, pokud jde o osobní zdravotní informace, a

h) systémová bezpečnostní data pro zdravotnické informační systémy, včetně dat řízení přístupu, a další data související s bezpečností konfigurace systému pro zdravotnické informační systémy.

Rozsah potřebné úrovně ochrany důvěrnosti, integrity a dostupnosti závisí na povaze informací, jejich použití a rizicích, kterým jsou vystaveny. Například statistické údaje (písm. c) výše) nemusí být důvěrné, ale ochrana jejich integrity může být velmi důležitá. Podobně jako data auditních záznamů (písm. g) výše) nevyžadují vysokou dostupnost (častá archivace s dobou pro vyhledání řádu spíše hodin, než vteřin by měla být pro danou aplikaci dostačující), ale jejich obsah by mohl být vysoce důvěrný. Hodnocení rizik umožňuje správně určit úroveň intenzity potřebné pro ochranu důvěrnosti, integrity a dostupnosti (viz B.4.4). Výsledky pravidelného posuzování rizik musí odpovídat prioritám a zdrojům organizace, která je provádí.

Hrozby a zranitelnosti bezpečnosti zdravotnických informací

Druhy ohrožení a zranitelnosti bezpečnosti informací se velice liší, stejně jako jejich popisy. I když žádný z nich není pro zdravotnictví specifický, co je však pro zdravotnictví specifické, je řada faktorů, které je třeba zvážit při posuzování hrozeb a zranitelností.

Vzhledem ke své povaze zdravotnické organizace fungují v takovém prostředí, kde přítomnost návštěvníků a široké veřejnosti nemůže být nikdy zcela vyloučena. Ve velkých zdravotnických organizacích je objem lidí pochybujících se provozními prostory značný. Tyto faktory zvyšují zranitelnost systémů vůči fyzickým hrozbám. Pravděpodobnost výskytu takových hrozeb se může zvýšit přítomností citově založených nebo duševně nemocných subjektů péče nebo jejich příbuzných.

Kritický význam správné identifikace subjektů péče a jejich správné porovnání s jejich lékařskými záznamy vede zdravotnické organizace ke sběru detailních identifikačních informací. Regionální registry pacientů a registry pacientů jiné jurisdikce (například registry subjektů péče) jsou někdy nejucelenější a nejaktuálnější úložiště identifikačních informací dostupných v jurisdikci. Tyto identifikační informace mají velkou potenciální hodnotu pro ty, kteří by je chtěli využít ke krádeži identity, a proto musí být důsledně chráněny.

Mnoho zdravotnických organizací je chronicky podfinancováno a jejich zaměstnanci někdy pracují pod značným stresem a se systémy, které jsou používány dlouho potom, co měly být vyřazeny. Tyto faktory mohou zvýšit potenciál určitých typů hrozeb a mohou zhoršit zranitelnosti. Na druhé straně klinická péče zahrnuje škálu odborných, technických, administrativních, pomocných a dobrovolných zaměstnanců, z nichž mnozí chápou svou práci jako poslání. Jejich obětavost a rozsah zkušeností mohou často účinně snížit vystavení se zranitelnostem. Vysoká úroveň odborné přípravy, kterou obdrží odborní pracovníci ve zdravotnictví, staví zdravotnictví do jiné pozice než mnoho jiných průmyslových odvětví při snižování výskytu vnitřních hrozeb.

Zdravotnickému prostředí, s jeho specifickými hrozbami a zranitelnostmi, je proto třeba věnovat zvláštní péči. Příloha A obsahuje informativní seznam typů hrozeb, které by měly být zdravotnickými organizacemi zváženy při posuzování rizik ve vztahu k důvěrnosti, integritě a dostupnosti zdravotnických informací a integritě a dostupnosti souvisících informačních systémů.

Kdo by měl číst tuto normu?

Tato norma je určena pro ty, kteří jsou zodpovědní za kontrolování bezpečnosti zdravotnických informací a pro zdravotnické organizace a další správce zdravotnických informací, hledající radu

k tomuto tématu, spolu s jejich bezpečnostními poradci, konzultanty, auditory, prodejci a třetími stranami poskytujícími služby.

Autoři této normy nemají v úmyslu psát učebnici počítačového zabezpečení, ani přepisovat to, co už bylo uvedeno v ISO/IEC 27001. Existuje mnoho bezpečnostních požadavků, které jsou společné pro všechny počítačové systémy, ať jsou používány v oblasti finančních služeb, výroby, řízení průmyslu nebo v jakémkoliv jiném organizovaném úsilí. Intenzivní úsilí se soustředilo na bezpečnostní požadavky, vyžadované specifickými výzvami při předávání elektronických zdravotnických informací, které podporují poskytnutí péče.

Výhody používání této normy

ISO/IEC 27002 je rozsáhlá a komplexní norma a její informace nejsou specificky uzpůsobené pro zdravotnictví. ISO 27799 umožňuje implementaci ISO/IEC 27002 do prostředí zdravotnictví konzistentním způsobem a se zvláštním zřetelem na specifické problémy, které sektor zdravotnictví představuje. Její implementace pomáhá zdravotnickým organizacím zajistit dodržování důvěrnosti a integrity dat v jejich péči, zachování dostupnosti kritických zdravotnických informačních systémů a prosazování odpovědnosti za zdravotnické informace.

Přijetí této normy zdravotnickými organizacemi jak uvnitř, tak i mezi jurisdikcemi přispěje k součinnosti a umožní bezpečné přijetí nově vznikajících technologií při poskytování zdravotní péče. Bezpečné a soukromí ochraňující sdílení informací může výrazně zlepšit lékařské výsledky.

V důsledku zavedení této normy mohou zdravotnické organizace očekávat snížení počtu a závažnosti jejich bezpečnostních incidentů, což umožní přesunout zdroje do produktivních činností. Bezpečnost IT pak umožní rozmístění zdravotnických prostředků rentabilním a efektivním způsobem. Průzkum provedený uznávaným Fórem bezpečnosti informací a tržními analytiky skutečně ukázal, že dobré všestranné zabezpečení může mít více než 2 % pozitivní dopad na výsledky organizace.

Konečně pak důsledný přístup k bezpečnosti IT, který je srozumitelný pro všechny zúčastněné ve zdravotní péči, povede ke zlepšení pracovní morálky a zvýšení důvěry veřejnosti v systémy, které spravují osobní zdravotní informace.

Jak používat tuto normu

Čtenářům, kteří ještě nejsou seznámeni s ISO/IEC 27002, se doporučuje, aby si nejprve přečetli úvodní část této normy, než budou pokračovat. Implementátoři ISO 27799 se musí nejdříve důkladně seznámit s ISO/IEC 27002, protože dále v textu je čtenář často odkazován na příslušné kapitoly této normy. Současná norma nemůže být plně pochopena bez přístupu k plnému znění ISO/IEC 27002.

Čtenáři hledající pokyny, jak implementovat ISO/IEC 27002 do zdravotnického prostředí, najdou praktický akční plán popsaný v příloze B. V této kapitole nejsou uvedeny žádné závazné požadavky. Místo toho jsou uvedeny obecné rady a pokyny, jak nejlépe provést implementaci ISO/IEC 27002 ve zdravotnictví. Kapitola je uspořádána v rámci cyklu aktivit (plánovat/dělat/kontrolovat/jednat), které jsou popsány v ISO/IEC 27001, a to, pokud bude dodrženo, povede k plné implementaci systému řízení bezpečnosti informací.

Čtenáři hledající specifickou radu ohledně kategorií bezpečnostních opatření a kapitol popsaných v ISO/IEC 27002 je naleznou v kapitolách této normy pod stejným číslem kapitoly a názvem, jak je uvedeno v ISO/IEC 27002. Tato kapitola povede čtenáře každou z jedenácti kapitol bezpečnostních opatření v ISO/IEC 27002. Tam, kde je to vhodné, jsou uvedeny minimální požadavky a v některých v případech jsou stanoveny pokyny pro správné zavedení bezpečnostních opatření dle ISO/IEC 27002 pro ochranu zdravotnických informací.

Po zavedení normy ISO/IEC 27002 je trvalé řízení považováno za zásadní, pokud výhody normy mají být zachovány. Kapitola 18 pojednává o posuzování shody a požadavcích na trvalé řízení bezpečnosti informací. Příloha C
obsahuje tabulku vlastního posuzování, pokud jde o shodu.

Tuto normu uzavírají čtyři informativní přílohy.

Příloha A popisuje obecné hrozby pro zdravotnické informace. Příloha B stručně popisuje praktický akční plán pro implementaci doplňujících norem týkajících se bezpečnosti informací. Příloha C obsahuje kontrolní seznam pro shodu s ISO 27799. Kapitola 2 obsahuje normy, které jsou citovány normativním způsobem; Bibliografie obsahuje další normy týkající se bezpečnosti zdravotnických informací.

1 Předmět normy

Tato norma poskytuje směrnice pro organizační normy bezpečnosti informací a postupy pro řízení bezpečnosti informací, včetně výběru, implementace a řízení opatření, s přihlédnutím k prostředí rizika (rizik) bezpečnosti informací organizace.

Tato norma definuje směrnice pro podporu interpretace a implementace zdravotnické informatiky ISO/IEC 27002 a je doprovodná k této normě.4)

Tato norma poskytuje pokyny k implementaci všech opatření uvedených v ISO/IEC 27002 a doplňuje je, kde je to nezbytné, aby mohly být efektivně použity pro řízení bezpečnosti informací ve zdravotnictví. Zavedením této normy budou zdravotnické organizace a ostatní správci zdravotnických informací schopni zajistit nezbytnou minimální úroveň zabezpečení, která odpovídá poměrům v organizaci a zachová důvěrnost, integritu a dostupnost osobních zdravotních informací v jejich péči.

Tato norma se vztahuje na zdravotnické informace ve všech jejich aspektech, bez ohledu na to, jakou má informace formu (slovní a číselnou, zvukové nahrávky, kresby, video a lékařské snímky), na prostředky k jejich ukládání (tisk nebo zápis na papíře nebo elektronické uložení) a na prostředky využívané k jejich přenosu (ručně, faxem, přes počítačové sítě nebo poštou), protože tyto informace musí být vždy náležitě chráněny.

Tato norma a ISO/IEC 27002 společně určují, jaké jsou požadavky na bezpečnost informací ve zdravotnictví, ale nedefinují, jak by měly být tyto požadavky splněny. To znamená, že tato norma je v co největším možném rozsahu technologicky neutrální. Neutralita ve vztahu k zavádění technologií je důležitým rysem. Bezpečnostní technologie stále prochází rychlým vývojem a jeho tempo se v současné době měří spíše v měsících než v letech. Oproti tomu mezinárodní normy, přestože jsou předmětem periodických revizí, by měly celkově zůstat v platnosti po celé roky. Důležité také je, že tato technologická neutralita umožňuje prodejcům a poskytovatelům služeb navrhovat nové a rozvíjející se služby, které budou splňovat nezbytné požadavky popsané v této normě.

Jak již bylo uvedeno v úvodu, dobrá znalost ISO/IEC 27002 je k pochopení této normy nezbytná.

Následující oblasti bezpečnosti informací jsou mimo rozsah této normy:

a) metodika a statistické testy pro efektivní anonymizaci osobních zdravotních informací;

b) metodika pro pseudonymizaci osobních zdravotních informací (viz Bibliografie pro stručný popis technické specifikace, která konkrétně pojednává o tomto tématu);

c) síť kvality služeb a metody pro měření dostupnosti sítí používaných pro zdravotnickou informatiku;

d) kvalita dat (na rozdíl od integrity dat).

Konec náhledu - text dále pokračuje v placené verzi ČSN.

1) Kromě zákonných povinností je k dispozici množství informací o etických povinnostech týkajících se zdravotnických informací, etický kodex Světové zdravotnické organizace. Tyto etické povinnosti mohou také mít za určitých okolností vliv na politiku bezpečnosti zdravotnických informací.

2) Je třeba poznamenat, že v některých zemích je řízení informací považováno za zabezpečení informací.

3) Úroveň dostupnosti záleží na použití, kde budou data uložena.

4) Tato norma je v souladu s revidovanou verzí ISO/IEC 27002.