ČESKÁ TECHNICKÁ NORMA

ICS 35.240.80 **Říjen 2013**

Zdravotnická informatika – Auditní záznamy elektronických zdravotních záznamů

ČSN
EN ISO 27789
98 2025

idt ISO 27789:2013

Health informatics – Audit trails for electronic health records

Informatique de santé – Historique d,expertise des dossiers de santé informatisés

Tato norma je českou verzí evropské normy EN ISO 27789:2013. 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 European Standard EN ISO 27789:2013. It was translated by the Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Národní předmluva

Informace o citovaných dokumentech

ISO 8601:2004 zavedená překladem v ČSN ISO 8601:2005 (98 2021) Datové prvky a formáty výměny – Výměna informací – Zobrazení data a času

EN ISO 27799:2008 zavedena překladem v ČSN EN ISO 27799:2010 (97 9739) Zdravotnická informatika – Systémy řízení bezpečnosti informací ve zdravotnictví využívající ISO/IEC 27002

Související ČSN

ČSN EN ISO 12052:2011 (98 2001) Zdravotnická informatika – Digitální zobrazování a komunikace v medicíně (DICOM), včetně pracovního postupu a správy dat

ČSN ISO/IEC 8824-1:2010 (36 9632) Informační technologie – Abstraktní syntaxe způsobu zápisu jedna (ASN.1): Specifikace základního způsobu zápisu

ČSN ISO/IEC 8824-2:2013 (36 9632) Informační technologie – Abstraktní syntaxe způsobu zápisu jedna (ASN.1): Specifikace informačního objektu

ČSN ISO/IEC 15408-2:2010 (36 9789) Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT – Část 2: Bezpečnostní funkční komponenty

ČSN ISO/IEC 2382-8:2001 (36 9001) Informační technologie – Slovník –- Část 8: Bezpečnost

ČSN ISO 7498-2:1993 (36 9615) Systémy na spracovanie informácií. Prepojenie otvorených systémov (OSI). Základný referenčný model. Část 2: Bezpečnostná architektúra

ČSN ISO/IEC 27000:2010 (36 9790) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník

ČSN IEC 60050-713:2000 (33 0050) Mezinárodní elektrotechnický slovník – Kapitola 713: Radiokomunikace: vysílače, přijímače, sítě a provoz

Vysvětlivky k textu převzatého dokumentu

Anglický termín „symbol“ se překládá českým slovem „symbol“, protože se zde používá ve významu nadřazeného termínu vůči podřazeným termínům: značky, znaky, označení atd., aby se všechny tyto termíny nemusely vypisovat.

Vypracování normy

Zpracovatel: Berkely Cert s. r. o., IČ 28882458, Ing. Daniel Kardoš, Ph.D.

Technická normalizační komise: TNK 20 Informační technologie

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

EVROPSKÁ NORMA EN ISO 27789
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM Březen 2013

ICS 35.240.80

Zdravotnická informatika – Auditní záznamy elektronických zdravotních záznamů
(ISO 27789:2013)

Health informations – Audit trails for electronic health records
(ISO 27789:2013)

Informatique de santé – Historique d,expertise des dossiers de santé informatisés
(ISO 27789:2013)

Medeizinische Informatik – Audit Trails für elektronische Gesundheitsakten
(ISO 27789:2013)

Tato evropská norma byla schválena CEN dne 16. února 2013.

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 bibliografické 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, 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, Španělska, Švédska, Švýcarska a Turecka.

CEN

Evropský výbor pro normalizaci

European Committee for Standardization

Comité Européen de Normalisation

Europäisches Komitee für Normung

Řídicí centrum: Avenue Marnix 17, B-1000 Brusel

Ref. č. EN ISO 27789:2013 E

Předmluva

Tento dokument (EN ISO 27789:2013) 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 září 2013 dát 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 září 2013.

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

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, Španělska, Švédska, Švýcarska a Turecka.

Oznámení o schválení

Text ISO 27789:2013 byl schválen CEN jako EN ISO 27789:2013 bez jakýchkoliv modifikací.

Obsah

Strana

Předmluva 4

Úvod 7

1 Předmět normy 9

2 Citované dokumenty 9

3 Termíny a definice 9

4 Symboly a zkratky 12

5 Požadavky a používání auditních dat 12

5.1 Etické a formální požadavky 12

5.1.1 Obecně 12

5.1.2 Politika přístupu 12

5.1.3 Jednoznačná identifikace uživatelů informačního systému 12

5.1.4 Uživatelské role 13

5.1.5 Bezpečné auditní záznamy 13

5.2 Používaní auditních dat 13

5.2.1 Řízení a dozor 13

5.2.2 Naplňování práv subjektů péče 13

5.2.3 Etický nebo právní doklad poskytovatele zdravotní péče o úkonu 13

6 Spouštěcí události 14

6.1 Obecně 14

6.2 Podrobnosti o typech událostí a jejich obsahu 14

6.2.1 Události přístupu k osobním zdravotním informacím 14

6.2.2 Dotazovací události k osobním zdravotním informacím 14

7 Podrobnosti auditního záznamu 15

7.1 Obecný formát záznamu 15

7.2 Identifikace spouštěcí události 16

7.2.1 ID události 16

7.2.2 Kód akce události 16

7.2.3 Datum a čas události 17

7.2.4 Indikátor závěru události 17

7.2.5 Kód typu události 17

7.3 Identifikace uživatele 18

7.3.1 ID uživatele 18

7.3.2 Alternativní ID uživatele 18

7.3.3 Jméno uživatele 18

7.3.4 Uživatel je žadatelem 18

7.3.5 Kód ID role 19

7.3.6 Účel použití 20

7.4 Identifikace přístupového bodu 21

7.4.1 Kód typu přístupového bodu sítě 21

7.4.2 ID přístupového bodu sítě 21

7.5 Identifikace auditního zdroje 21

7.5.1 Přehled 21

Strana

7.5.2 ID místa auditní organizace 22

7.5.3 ID auditního zdroje 22

7.5.4 Kód typu auditního zdroje 22

7.6 Identifikace zúčastněného objektu 23

7.6.1 Přehled 23

7.6.2 Kód typu zúčastněného objektu 23

7.6.3 Kód typu role zúčastněného objektu 24

7.6.4 Životní cyklus dat zúčastněného objektu 24

7.6.5 Kód typu ID zúčastněného objektu 25

7.6.6 PolicySet povolení zúčastněného objektu 26

7.6.7 Citlivost zúčastněného objektu 26

7.6.8 ID zúčastněného objektu 26

7.6.9 Jméno zúčastněného objektu 27

7.6.10 Dotaz zúčastněného objektu 27

7.6.11 Podrobnosti zúčastněného objektu 27

8 Auditní záznamy jednotlivých událostí 27

8.1 Události přístupu 27

8.2 Dotazovací události 29

9 Řízení bezpečnosti auditních dat 30

9.1 Bezpečnostní úvahy 30

9.2 Zajištění dostupnosti auditního systému 31

9.3 Požadavky uchovávání 31

9.4 Zajištění důvěrnosti a integrity auditních záznamů 31

9.5 Přístup k auditním datům 31

Příloha A (informativní) Auditní scénáře 32

Příloha B (informativní) Služby auditního logu 37

Bibliografie 44

Úvod

0.1 Obecně

Osobní zdravotní informace jsou mnohými považovány za nejdůvěrnější ze všech typů osobních informací a ochrana jejich důvěrnosti je základem pokud soukromí subjektu péče má být udržováno. Za účelem ochrany konzistence zdravotních informací, je také důležité, aby celý jejich životní cyklus byl plně auditovatelný. Zdravotní záznamy mají být vytvořené, zpracované a řízené způsobem, který zaručí integritu a důvěrnost jejich obsahu a podporu zákonných požadavků subjektu péče při jejich vytváření, používaní a udržování.

Důvěra k elektronickým zdravotním záznamům vyžaduje fyzické a technické bezpečnostní prvky společně s prvky integrity dat. Mezi nejdůležitější ze všech bezpečnostních požadavků k ochraně zdravotních informací a integrity záznamů patři ty, které se týkají auditu a logování. Ty pomáhají k zabezpečení prokazatelnosti odpovědnosti pro subjekty péče, které svěří své informace systémům elektronických zdravotních záznamů (EHR). Také pomáhají chránit integritu záznamu, neboť poskytují silnou motivaci uživatelům takových systémů, aby dodržel zásady organizace o používání těchto systémů.

Efektivní audit a protokolování mohou pomáhat odhalit zneužití systémů EHR nebo dat EHR a mohou pomoci organizacím a subjektům péče získat odškodnění od uživatelů zneužívajících svá práva. Pro efektivní audit jsou nezbytné auditní záznamy obsahující dostatečné informace k řešení širokého spektra možných situací (viz
Příloha A)

Auditní logy jsou doplňkem k řízení přístupu. Auditní logy poskytují prostředek posouzení shody s politikou přístupu organizace a mohou přispět ke zlepšení a zpřesnění politiky samotné. Ale tato politika musí rovněž počítat s výskytem neočekávaných nebo havarijních případů, analýza auditních protokolů se proto stává primárním prostředkem pro zabezpečení řízení přístupu.

Tato mezinárodní norma je striktně zaměřena, na logování událostí. Předpokládá se, že změny hodnot dat v polích EHR budou zaznamenány v samotném databázovém systému EHR a ne v auditním logu. Předpokládáme, že sám systém EHR obsahuje jak předcházející, tak rovněž aktualizované hodnoty každého pole. To je v souladu se současným přístupem k architektuře databází na principu „bodu v čase“. Předpokládáme, že auditní log sám o sobě nebude obsahovat žádné osobní zdravotní

informace, kromě identifikačních údajů a vazeb k záznamu.

Elektronické zdravotní záznamy jedné osoby mohou být v rámci mnoha různých informačních systémů a napříč organizacemi nebo hranicemi jurisdikcí. Ke sledování všech akcí zahrnujících záznamy jednoho subjektu péče je nezbytným předpokladem společný rámec. Tato mezinárodní norma poskytuje takový rámec. K podpoře auditních záznamů napříč různými doménami je nezbytné zahrnout doporučení v tomto rámci do politik, které specifikují vnitřní požadavky domény, jako jsou pravidla řízení přístupu a lhůty uchovávání. Doménové politiky mohou být odkazovány implicitně identifikací zdroje auditního logu.

0.2 Přínos použití této mezinárodní normy

Normalizace auditních záznamů elektronických zdravotních záznamů má dva cíle:

- zachycení informací v auditním logu postačujících k tomu, aby jasně rekonstruovaly detailní chronologii událostí, které formovaly obsah elektronického zdravotního záznamu, a
- zabezpečení toho, aby auditní záznam akce, týkající se záznamu subjektu péče, mohl být spolehlivě sledován napříč organizačními doménami.

Tato mezinárodní norma je určená těm, kdo jsou odpovědní za dohled nad bezpečností zdravotnických informací nebo ochranou soukromí a organizacím zdravotní péče a osobám odpovědným za hledání pomoci v auditních záznamech zdravotnických informací, společně s jejich bezpečnostními experty, konzultanty, auditory, dodavateli a třetími stranami poskytovatelů služeb.

0.3 Srovnání se souvisejícími normami auditních záznamů elektronických zdravotních záznamů

Tato mezinárodní norma je v souladu s požadavky ISO 27799:2008, které souvisí s auditováním a auditními záznamy.

Některým čtenářům může být známa Komise techniky Internetu (Engineering Task Force (IETF) Request for Comment (RFC) 3881.[13] (Čtenáři, kteří nejsou obeznámeni s IETF RFC 3881, nemusí tento dokument vyhledat, jelikož jeho znalost není potřebná k porozumění této mezinárodní normy.) Informační RFC 3881, datovaná 2004-09, jež se nadále nevyskytuje jako platná v databázi IETF byla prvním užitečným pokusem o specifikování obsahu auditních logů ve zdravotnictví. Pokud je to možné, tato mezinárodní norma vychází a je v souladu se započatou prací v RFC 3881 a zohledňuje přístup k EHR.

0.4 Poznámka k terminologii

Několik blízce souvisejících termínů je definováno v kapitole 3. *Auditní log* je chronologická sekvence *auditních záznamů*; každý auditní záznam obsahuje důkaz přímo se týkající a vyplývající z výkonu postupů nebo funkce. Jelikož systémy EHR mohou být komplexním seskupením systémů a databází, může existovat více než jeden auditní log obsahující informace o systémových událostech, které vedly ke změně EHR subjektu péče. Ačkoli termíny *auditní záznamy* a *auditní log* jsou často používány zaměnitelně, v této mezinárodní normě termínu *auditní záznamy* odpovídá soubor všech auditních záznamů z jednoho nebo více auditních logů, které odkazují na specifický subjekt péče nebo specifický elektronický zdravotní záznam nebo specifického uživatele. *Auditní systém* poskytuje všechny nezbytné funkce zpracování informací k údržbě jednoho nebo více auditních logů.

1 Předmět normy

Tato mezinárodní norma specifikuje společný rámec pro auditní záznamy elektronických zdravotních záznamů (EHR), pokud jde o události spouštění auditu a dat auditu, aby úplnost souboru osobních zdravotnických informací byla auditovatelná napříč informačními systémy a doménami.

Je vhodná pro systémy zpracování osobních zdravotních informací, které v souladu s ISO 27799 vytvářejí bezpečnostní auditní záznam vždy, když uživatel připravuje k vytváření, aktualizaci nebo archivaci osobní zdravotní informace pomocí systému.

POZNÁMKA Tyto auditní záznamy přinejmenším jednoznačně identifikují uživatele, jednoznačně identifikují subjekt péče, identifikují činnosti vykonávané uživatelem (vytvoření záznamu, přístup, aktualizaci atd.), a zaznamenávají datum a čas výkonu činnosti.

Tato mezinárodní norma pokrývá pouze činnosti vykonávané s EHR, které jsou řízené politikou přístupu v oblasti výskytu elektronického zdravotního záznamu. Nejedná se o jiné osobní zdravotní informace z elektronického zdravotního záznamu, než jsou auditní záznamy obsahující propojení na segment EHR jak je definuje politika řízení přístupu.

Nepokrývá specifikaci a použití auditních logů pro účely řízení a systému bezpečnosti, jako je detekce problémů výkonu, chyby aplikace nebo podporu obnovy dat, které řeší obecné normy počítačové bezpečnosti jako je ISO/IEC 15408-2.[9]

Příloha A obsahuje příklady auditních scénářů. Příloha B obsahuje celkový přehled služeb auditních logů.