ČESKÁ TECHNICKÁ NORMA

ICS 35.240.80 **Srpen 2010**

Zdravotnická informatika – Přenos elektronických zdravotních záznamů – Část 4: Bezpečnost

ČSN EN 13606- 4
98 1015

Health informatics – Electronic health record communication – Part 4: Security

Medizinische Informatik – Kommunikation von Patientendaten in elektronischer Form – Teil 4: Sicherheit

Informatique de santé – Dossiers de santé informatisés communicants – Partie 4: Exigences de sécurité et regles de distribution

Tato norma je českou verzí evropské normy EN 13606-4:2007. 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 13606-4:2007. It was translated by Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN EN 13606-4 (98 1015) ze října 2007.

Národní předmluva

Změny proti předchozím normám

Proti předchozí normě dochází ke změně způsobu převzetí EN 13606-4:2007 do soustavy norem ČSN. Zatímco ČSN EN 13606-4 z října 2007 převzala EN 13606-4:2007 oznámením ve Věstníku jako ČSN, tato norma ji přejímá překladem.

Souvisící ČSN

ČSN P ENV 13608-1:2001 (98 2014) Zdravotnická informatika – Bezpečnost komunikace ve zdravotnictví – Část 1: Pojmy a terminologie

ČSN P ENV 13608-2:2002 (98 2014) Zdravotnická informatika – Zabezpečené komunikace ve zdravotnictví – Část 2: Zabezpečené datové objekty

ČSN P ENV 13608-3:2002 (98 2014) Zdravotnická informatika – Zabezpečené komunikace ve zdravotnictví – Část 3: Zabezpečené datové kanály

ČSN EN 14484:2004 (98 1024) Zdravotnická informatika – Mezinárodní přenos dat o zdravotním stavu osob podle Směrnice EU o ochraně dat – Politika zabezpečení na vysoké úrovni

ČSN EN 14485:2004 (98 1025) Zdravotnická informatika – Návod pro zprostředkování dat o zdravotním stavu osob v mezinárodních aplikacích v kontextu se Směrnicí EU o ochraně dat

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 17799:2006 (36 9790) Informační technologie – Bezpečnostní techniky – Soubor postupů pro management bezpečnosti informací

ČSN EN ISO 27799:2010 (98 2021) Zdravotnická informatika – Management bezpečnosti informací ve zdravotnictví využívající ISO/IEC 27002 (ISO 27799:2008)

Vysvětlivky k textu převzaté normy

V této normě je v případě množného čísla anglických zkratek a výrazů ponecháno značení uvedené v originálu normy, tj. malé písmeno s (například RECORD_COMPONENTs).

Pro účely této normy je anglický termín generic překládán jako generický. Anglický termín "communication" se překládá jako přenos, sdílení nebo komunikace. Anglický termín "*encounter*" je přeložen jako (osobní) kontakt. Anglický termín "audit log" je přeložen jako auditní záznam.

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.

Pro účely této normy je anglický termín "*federated*" přeložen jako federovaný. Federovaný model elektronického zdravotního záznamu integrované péče je model systému sdíleného EHR, kdy je EHR integrované péče sestaven v reálném čase, tedy když je požadován, na rozdíl od konsolidovaného modelu elektronického zdravotního záznamu integrované péče, kdy je EHR integrované péče sestaven při jeho tvorbě a aktualizaci.

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČO 61470716

Technická normalizační komise: TNK 20 Informační technologie

Pracovník Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Ing. Petr Wallenfels

EVROPSKÁ NORMA EN 13606-4
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM Březen 2007

ICS 35.240.80 Nahrazuje ENV 13606-4:2000

**Zdravotnická informatika – Přenos elektronických zdravotních záznamů –
Část 4: Bezpečnost**

Health informatics – Electronic health record communication –
Part 4: Security

Informatique de santé – Dossiers de santé informatisés communicants –
Partie 4: Exigences de sécurité et regles de distribution

Medizinische Informatik – Kommunikation von Patientendaten in elektronischer Form –
Teil 4: Sicherheit

Tato evropská norma byla schválena CEN 10. února 2007.

Členové CEN jsou povinni splnit Vnitřní předpisy CEN/CENELEC, v nichž jsou stanoveny podmínky, za kterých se musí této evropské normě bez jakýchkoliv modifikací dát status národní normy. Aktualizované seznamy a bibliografické citace týkající se těchto národních norem lze obdržet na vyžádání v Řídicím centru 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, má stejný status jako oficiální verze.

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

CEN

Evropský výbor pro normalizaci

European Committee for Standardization

Comité Européen de Normalisation

Europäisches Komitee für Normung

Řídicí centrum: rue de Stassart, B-1050 Brusel

Ref. č. EN 13606-4:2007 E

Obsah

Strana

Předmluva

Tento dokument (EN 13606-4:2007) byl připraven technickou komisí CEN/TC 251 „Zdravotnická informatika“, jejíž sekretariát zajišťuje NEN.

Této evropské normě musí být udělen status národní normy, buďto zveřejněním identického textu nebo schválením nejpozději do září 2007, a nekompatibilní národní normy musí být vyřazeny nejpozději do září 2007.

Tento dokument nahrazuje ENV 13606-4:2000.

V souladu s vnitřními předpisy CEN/CENELEC jsou národní normalizační organizace následujících zemí zavázáni implementovat tuto evropskou normu: Belgie, Bulharska, České republiky, Dánska, Estonska, Finska, Francie, Irska, Islandu, Itálie, Kypru, Litvy, Lotyšska, Lucemburska, Maďarska, Malty, Německa, Nizozemska, Norska, Polska, Portugalska, Rakouska, Rumunska, Řecka, Slovenska, Slovinska, Spojeného království, Španělska, Švédska a Švýcarska.

Úvod

Výzva obsažená v této dílčí normě

Přenos elektronických zdravotních záznamů (Electronic Health Records (EHRs)) jako celek nebo po jednotlivých částech, v rámci a napříč organizacemi, a někdy napříč národními hranicemi je výzvou z pohledu bezpečnosti. Zdravotní záznamy by měly být vytvářeny, zpracovávány a řízeny způsobem, který zaručuje důvěrnost jejich obsahu a opravňuje kontrolu prováděnou pacienty v tom, jak jsou používány. Na celém světě se tyto principy postupně pečlivě začleňují do národní legislativy na

ochranu dat. Směrnice EU na ochranu dat [95/46/EC] a Doporučení Rady Evropy o ochraně zdravotních dat R(97)5 poskytují důležitý právní základ pro doporučení pro bezpečnostní služby podle popisu v této normě. Tyto listiny prohlašují, že subjekt péče má právo hrát hlavní roli při rozhodnutích o obsahu a distribuci svého elektronického zdravotního záznamu stejně jako právo být informován o jeho obsahu. Přenos informací zdravotního záznamu třetím stranám by měl proběhnout pouze se souhlasem pacienta (což může být „jakékoliv svobodně dané specifické a informované označení jeho přání, kterým subjekt dat projevuje svůj souhlas se zpracováním osobních dat s ním souvisících"). Pro mezinárodní přenosy zdravotních záznamů poskytují EN 14484 (Zdravotnická informatika – Mezinárodní přenos osobních zdravotních dat, o kterých pojednává Směrnice EU na ochranu dat – Bezpečnostní politika vyšší úrovně) a EN 14485 (Zdravotnická informatika – Návod pro nakládání s osobními zdravotními daty v mezinárodních aplikacích v kontextu Směrnice EU na ochranu dat) návod pro politiku, jak toto může být zákonně a bezpečně provedeno.

V ideálním případě by měla být každá podrobná položka v záznamu pacienta schopná propojení se seznamem řízení přístupu osob, které mají právo prohlédnout si ty informace, které byly vygenerovány nebo alespoň odsouhlaseny pacientem a které odrážejí dynamickou povahu skupiny osob s legitimní povinností péče ve vztahu k pacientovi během jeho života. Seznam řízení přístupu bude v ideálním případě obsahovat také ty osoby, které mají práva přistupovat k datům z jiných důvodů, než z povinnosti péče (například řízení zdravotnických služeb, epidemiologie a veřejné zdraví, povolený výzkum), ale vylučují jakékoliv informace, které nemusí vidět nebo které podle mínění pacienta jsou příliš osobní na to, aby k nim měli přístup. Na druhé straně označování informací pacienty nebo jejich zplnomocněnými zástupci jako osobní nebo privátní by pokud možno nemělo bránit těm, kdo legitimně potřebují mít k informacím v naléhavých případech přístup, ani by nemělo náhodně mít za následek, že by původní poskytovatelé zdravotní péče měli tak filtrovaný pohled, že budou uvedeni v omyl a budou pacienta řídit nevhodně. Náhledy pacientů na vlastní citlivost položek v jejich zdravotním záznamu se mohou v průběhu času vyvíjet s tím, jak se mění jejich osobní obavy o zdraví nebo jak se mění sociální přístupy ke zdravotním problémům. Pacienti by si možná přáli nabídnout určité heterogenní úrovně přístupu rodině, přátelům, opatrovníkům a členům jejich komunity. Rodiny si možná přejí poskytnout prostředky, kterými budou schopny přistupovat k částem svých záznamů navzájem (ale ne nutně ve stejném rozsahu), aby monitorovaly vývoj zděděných podmínek uvnitř stromu rodiny.

Taková sada požadavků je pravděpodobně rozsáhlejší než požadavky ochránců dat ve většině dalších průmyslových odvětví. V praxi je to dosaženo velice složitě díky:

- počtu položek zdravotních záznamů provedených u pacienta v průběhu moderní zdravotní péče;
- počtu zaměstnanců zdravotní péče, často se střídajících na pracovních pozicích, kteří by mohli potenciálně v jednotlivých případech přijít do styku s pacientem;
- počtu organizací, s kterými by pacient mohl přijít do styku během svého života;
- obtížnosti (pro pacienta nebo pro kohokoliv jiného) standardně provedené klasifikace toho, jak citlivá by mohla být položka záznamu;
- obtížnosti určení, jak významná by mohla být jednotlivá položka zdravotního záznamu pro budoucí péči o pacienta, a pro které třídy uživatele;
- logicky neodstranitelné povaze EHR a potřebě přezkoumání přístupových oprávnění, která by měla být vedená stejně přísně, jako přezkoumání samotných položek EHR;
- potřebě určit příslušný přístup velmi rychle, v reálném čase, a potenciálně v distribuovaném výpočetním prostředí;
- vysoké úrovní zájmu, vyjádřeného rostoucí menšinou pacientů, u kterých je jejich souhlas se zveřejněním zaznamenaný a respektovaný;
- nízké úrovni zájmu, kterou má většina pacientů o těchto požadavcích, což historicky omezilo prioritu a investice poskytnuté k vypořádání se s tímto aspektem přenosu EHR.

Za účelem podpory interoperabilních EHRs a bezproblémového přenosu dat EHR mezi poskytovateli

zdravotní péče je třeba, aby byl proces vyjednávání potřebný k rozhodnutí, zda smějí být danému žadateli data EHR poskytnuta, schopný automatizace. Pokud by to nebylo možné, prodlevy a pracovní zátěž spojená s managementem „lidských“ rozhodnutí pro veškerou nebo většinu komunikace by snižovaly hodnotu dosažitelnou interoperabilitou dat.

Hlavní zásady postoje k vývoji norem v oblasti řízení přístupu v přenosech EHR by měly vyhovovat charakteristikám a parametrům žádosti o politiky poskytovatelů EHR a jakémukoliv řízení přístupu nebo vyjádření souhlasu v rámci specifikovaného EHR, aby se uchoval příslušný důkaz o zpřístupnění a aby bylo možné automatizované zpracování.

V praxi probíhají snahy vyvinout mezinárodní normy pro definování takových systémů řízení přístupu a řízení privilegií, které by byly schopny vyjednávání na úrovni počítač – počítač. Tento způsob činnosti je však připisován zdravotním službám, které se dohodly na vzájemném konzistentním rámci pro definování privilegií, která chtějí přidělit zaměstnancům, a na škále citlivosti, kterou nabízejí pacientům k definování v rámci jejich EHRs.

To vyžaduje konzistenci ve způsobu, jakým je příslušná informace vyjádřena, aby bylo možné tento proces účelně měřit v definovaném čase (když jsou přidávány nové položky EHR), v runtimu (když je celý EHR vyhledáván nebo dotazován), a trvale po celou dobu života pacienta. Je také důležité rozpoznat, že v dlouhodobém výhledu bude v rámci Evropy narůstat různorodost ve specifických přístupech k zabezpečování přenosů EHR, včetně odchylné legislativy, a že přístup k normalizaci cestou strohého nařizování není v současné době možný.

Tato evropská norma tedy nepředepisuje vlastní pravidla přístupu (tj. nespecifikuje, kdo by měl mít přístup k čemu a pomocí jakých bezpečnostních mechanismů); ta musí být stanovena uživatelskými komunitami, národními směrnicemi a legislativou. Definuje však základní rámec, který může být použit jako minimální specifikace politiky přístupu k EHR, a bohatší generické zobrazení pro přenos jemnějších podrobných informací o politice. Tento rámec doplňuje celkovou architekturu definovanou v části 1 této vícedílné normy a definuje specifické informační struktury, které mají být komunikovány jako část EHR_EXTRACT definované v části 1.

POZNÁMKA Některé druhy dohod nutných pro bezpečnost přenosu EHR spadají nutně mimo rozsah této normy. Úplná ochrana přenosu EHR vyžaduje věnovat pozornost velkému počtu problémů, z nichž mnohé nejsou specifické pro zdravotní informace. CEN/TC 251/WG III vyvinula sérii norem souvisících s bezpečnostními službami a řízením bezpečnosti v oblasti zdravotní péče, které by měly být použity při budování systémů EHR. Mnoho z této práce se nyní provádí ve spolupráci mezi CEN a ISO/TC 215/WG 4 Zdravotnická informatika/Bezpečnost. Existuje mnoho rozpracovaných pracovních položek, které nebyly v době vypracování tohoto návrhu normy publikovány, ale které by mohly být dostupné před publikací této normy a užitečné pro implementátory systémů EHR. Uvádíme některé z nich:

- Joint CEN-ISO Work Item: ISO/TS 22600 Privilege Management and Access Control (PMAC) (Společná pracovní položka CEN-ISO: ISO/TS 22600 Správa privilegií a řízení přístupu),
- ISO Work Item: ISO/TS 21298 on Functional and Structural roles (Pracovní položka ISO ISO/TS 21298 o funkčních a strukturálních rolích)

Scénáře přenosu

Modely rozhraní a zpráv požadované k podpoře přenosu EHR jsou předmětem části 5 této vícedílné normy. Zde uvedený popis je přehledem procesu přenosu s cílem ukázat interakce, u kterých jsou nutné bezpečnostní rysy. Dále uvedený diagram znázorňuje hlavní toky dat a scénáře, které musí vzít tato norma v úvahu. U každého hlavního toku dat bude existovat odezva na přijetí, a volitelně může být vráceno odmítnutí místo požadovaných dat.

Obrázek 1 – Základní toky dat a obchodní procesy souvisící s bezpečností, jimiž se tato dílčí norma zabývá

Žadatelem o EHR, Příjemcem EHR a Revizorem auditního záznamu by mohli být odborníci na lékařskou péči, pacient, zákonný zástupce nebo jiná strana s dostatečnou autorizací pro přístup k informacím o zdravotní péči. Jak EHR_EXTRACT tak auditní záznam, jestliže jsou poskytovány, mohou být filtrovány, aby se omezilo zpřístupnění tak, aby odpovídalo privilegiím příjemce. O tomto aspektu řízení přístupu je pojednáno dále v této úvodní části.

Žádost o data EHR

Tato výměna informací není vždy vyžadována (například data EHR mohou být předána od Poskytovatele k Příjemci jako v případě propouštěcí zprávy). Rozhraní žádosti vyžaduje zahrnout dostatečný profil Žadatele, aby Poskytovatel EHR byl schopen učinit rozhodnutí o přístupu, rozšířit auditní záznam a poskytnout příslušná data zamýšlenému Příjemci. V některých případech by Žadatel o EHR nemusel být stejnou stranou jako Příjemce EHR – například softwarový agent by mohl aktivovat sdělení obsahující data EHR určená k odeslání odborníkovi na zdravotní péči. V takových případech jsou to pověřovací listiny (pověření) Příjemce EHR, které stanoví zejména rozhodnutí o přístupu, které má být provedeno.

Žádost o EHR může vyžadovat zahrnutí souhlasu k přístupu nebo odkaz na něj a pověření k péči, například poskytnutím některé formy explicitního souhlasu od pacienta nebo nařízením péče.

Vyjednávání mezi Žadatelem a Poskytovatelem dat EHR bude stale více automatizováno a informace zahrnuté v této interakci musí postačovat k tomu, aby umožnily vyjednávací politiku plně automatizovanou pomocí počítače.

Požadavky na tuto interakci budou reflektovány v modelu rozhraní EHR_Request definovaném v části 5 této normy.

Potvrzení přijetí EHR_Request

Žádné jedinečné bezpečnostní faktory.

Uskutečnění rozhodnutí o přístupu, filtrace dat EHR

Při zpracování žádosti o EHR je při určení, jaká data jsou extrahována z cílového EHR nutné vzít v úvahu politiky patřící Poskytovateli EHR a politiky přístupu v samotném EHR. Tato dílčí norma nemůže předepisovat souhrnnou množinu politik, potenciálně odvozených z národní, regionální, pro organizace specifické, odborné nebo jiné legislativy, které mohou ovlivnit Poskytovatele EHR.

Tato dílčí norma však definuje celkový rámec pro vyjádření politik přístupu na principu interoperability, které by se mohly vztahovat k jakémukoliv jednotlivému EHR, vytvořenému pacientem nebo jeho zástupci. Takové politiky by nebyly uloženy v systému fyzického EHR tímto způsobem; mohly by být místo toho například integrovány do serveru pro politiku přístupu propojeného se serverem EHR.

Tímto rozhodnutím o přístupu se zabývá podrobněji kapitola 6 této dílčí normy.

Zamítnutí EHR_EXTRACT

Jestliže má být rozhodnutí o přístupu odmítnuto, je nutné definovat v hrubší struktuře soubor příčin, aby byl zformován vhodný soubor obsahující odezvy od Poskytovatele EHR. Je však důležité, aby odmítnutí a jakýkoliv udaný důvod příjemci nenaznačoval, že požadovaná data EHR existují – dokonce i odhalení samotné jejich existence by mohlo být pro pacienta škodlivé.

Žádné jedinečné bezpečnostní faktory – model rozhraní bude definován v části 5 této normy.

Poskytnutí EHR_EXTRACT

Je nutné poznamenat, že Příjemce EHR nemusí být totožný se Žadatelem o EHR, a poskytnutí EHR nemusí být ve skutečnosti aktivováno žádostí. Místo toho by mohlo být iniciováno poskytovatelem jako součást poskytování sdílené péče nebo přidání nových dat k existujícímu EHR.

Požaduje se, aby EHR_EXTRACT odpovídala Referenčnímu modelu definovanému v části 1 této normy a modelu rozhraní definovanému v části 5 této normy.

EHR_EXTRACT musí obsahovat jakékoliv příslušné politiky přístupu vyjadřované ve shodě s touto dílčí normou, které mají řídit jakékoliv další předávání komunikovaných dat EHR, nebo na ně odkazovat. Politiky mohou být pouze předmětem odkazu v případě, že je o příjemci EHR známo, že má přímý přístup k téže informaci jinými prostředky.

Potvrzení přijetí EHR_EXTRACT

Žádné jedinečné bezpečnostní faktory.

Generování položky záznamu (logu) o přístupu k EHR

Je to praxe předpokládaná v jakémkoliv systému EHR, ale není specifikovaná jako normativní rozhraní, z důvodu odlišných přístupů a schopností současných systémů.

U systémů vnitřního auditu v systému EHR není vyžadována interoperabilita vyjma podpory níže uvedených rozhraní.

Žádost o náhled záznamu o přístupu k EHR

V současné době je tato žádost pokládána za žádoucí praxi, aby umožnila pacientovi zjistit, kdo měl v distribuovaném výpočetním prostředí přístup k části nebo k celému jeho EHR. Předmětem tohoto rozhraní podle definice v této normě je požádat o náhled auditního záznamu, který informuje příjemce o tom, kdo uskutečnil přístup ke které části daného EHR a kdy. Cílem tohoto rozhraní není podporovat situace, kdy je požadována úplná prohlídka auditního záznamu pro právní účely nebo pro jiná vyšetřování. O tomto rozhraní je pojednáno v kapitole 6 této části normy.

Model rozhraní bude definován v části 5 této normy.

Poskytnutí náhledu záznamu o přístupu k EHR

Je to žádoucí praxe a požaduje interoperabilní znázornění takové položky (nebo množiny položek). O tomto rozhraní je pojednáno v kapitole 6 této dílčí normy.

Ačkoliv soudní vyšetřování bude požadovat, aby byl auditní záznam poskytnut v kompletní a nezměněné podobě, předložení náhledu auditního záznamu pacientovi nebo odborníku na zdravotní péči by mohlo vyžadovat, aby některé položky byly odfiltrovány (například ty položky, které se odkazují na data EHR, ke kterým pacient nemá přístup).

Model rozhraní bude definován v části 5 této normy.

Zamítnutí náhledu záznamu o přístupu k EHR

Jestliže nemá být žádosti vyhověno, je nutné definovat v hrubší struktuře soubor příčin. Je však důležité, aby pro příjemce ze zamítnutí a jakéhokoliv udaného důvodu nevyplývalo, že požadovaná data EHR existují – dokonce i odhalení samotné jejich existence by mohlo být pro pacienta škodlivé.

Žádné jedinečné bezpečnostní faktory – model rozhraní bude definován v části 5 této normy.

Potvrzení přijetí náhledu záznamu o přístupu k EHR

Žádné jedinečné bezpečnostní faktory.

Požadavky a technický přístup

Představou výzkumu, průmyslových odvětví a dřívějších evropských norem o komunikaci interoperabilních elektronických zdravotních záznamů bylo umožnit, aby si odlišné klinické systémy mohly vyměňovat celé EHR pacienta nebo jeho části standardním způsobem, který může přesně a obecně znázorňovat hodnoty dat, kontextovou organizaci a k lékařství i právu se vztahující místo původu informace v jakémkoliv vzniklém systému EHR. Citlivé informace, například informace v systémech EHR, musí být zaznamenány, uloženy, zpracovány a komunikovány bezpečným a důvěryhodným způsobem. Přenos EHR musí proto také splňovat určité bezpečnostní požadavky, například:

- autentizaci entit (lidí, softwaru, zařízení atd.), které by mohly legitimně požadovat nebo poskytovat data EHR;
- autorizaci, správu privilegií a řízení přístupu;
- integritu informací EHR, které jsou ukládány, zpracovávány a komunikovány;
- bezpečnostní klasifikaci informací EHR;
- definici, projednání a propojení politik mezi entitami, které požadují a poskytují data EHR;
- auditovatelnost a sledovatelnost informací, ke kterým je přistupováno, které jsou zpracovávány a komunikovány;
- souhrnné zabezpečovací postupy a postupy pro zajištění kvality.

Dosavadní práce evropského výzkumu a vývoje (R&D) v těchto oborech zahrnuje projekty jako je SEISMED, TrustHealth a HARP.

Většina informačních systémů organizací zabývajících se zdravotní péčí již má zavedeny bezpečnostní systémy a služby, aby chránila širokou škálu toků dat souvisících se zdravím, čehož jsou přenosy EHR pouze jedním příkladem. Kromě toho oblast bezpečnosti zdravotnických informací aktivně vyvíjí generické přístupy ke specifikování, implementování, profilování a hodnocení stále se zlepšujících bezpečnostních služeb. Mnoho požadavků, které patří ke přenosům EHR, je proto také aplikovatelných na všechny komunikace v oblasti zdravotní péče.

Generické bezpečnostní požadavky v oblasti zdravotní péče

Nejšířeji akceptované požadavky na celkový bezpečnostní přístup v oblastech, kde se pracuje s citlivými a osobními údaji, jsou zveřejněny v ISO/IEC 17799. Tato norma specifikuje druhy opatření, které by měly být přijaty na ochranu takových aktiv, jako jsou data EHR, a způsoby, jakými by měla být taková data bezpečně komunikována jako součást distribuovaného výpočetního prostředí. Návod pro oblast zdraví k této všeobecné normě byl vyvinut organizací ISO ve spolupráci s CEN (ISO/DIS 27799) Zdravotnická informatika – Management bezpečnosti informací ve zdravotnictví využívající

ISO/IEC 17799. Tento návod usnadní formulaci obecných bezpečnostních politik v celé oblasti zdravotní péče a měl by pomoci podporovat zavedení interoperabilních bezpečnostních komponent a služeb.

Pro přenos EHR přes hranice také do zemí mimo Evropskou Unii jsou návod a specifikace bezpečnostní politiky obsaženy v EN 14484 (Zdravotnická informatika – Mezinárodní přenos osobních zdravotních dat pokrytý směrnicí EU na ochranu osobních dat – Bezpečnostní politika vyšší úrovně (International transfer of personal health data covered by the EU data protection directive – High Level Security Policy)) a EN 14485 (Zdravotnická informatika – Návod pro nakládání s osobními zdravotními daty v mezinárodních aplikacích v kontextu směrnice EU na ochranu osobních dat (Health informatics – Guidance for handling personal health data in international applications in the context of the EU data protection directive)). ISO 22857 poskytuje obdobné informace v případě, že nejde o země EU.

Přesné bezpečnostní požadavky, které musí být splněny, aby mohla být povolena jakákoliv komunikační instance EHR, budou řízeny mnoha národními a místními politikami jak odesílající tak přijímající strany, a v jakýchkoliv mezilehlých spojeních v komunikačním řetězci. Mnoho z těchto politik bude aplikováno na komunikace v oblasti zdravotní péče obecně, a bude se lišit mezi zeměmi a klinickými prostředími způsoby, které nemohou a neměly by být usměrňovány touto normou.

Například jakýkoliv přístup k datům EHR bude vyžadovat, aby žádající strana byla adekvátně autentizována tak, aby příslušný subjekt byl autorizován k podání žádosti a aby, je-li žádosti vyhověno, nominovaný příjemce dat EHR (což nemusí být vždy žadatel) byl autorizován k přijetí dat. Všechny přenosy se musí uskutečnit přes chráněné sítě a musí být uchováván auditní záznam všech toků dat EHR. Infrastruktura k poskytnutí těchto bezpečnostních služeb bude obecně použitelná pro mnoho bezpečných domén, nejen pro zdravotní péči, a tato norma předpokládá, že tyto služby budou zavedeny a používány v každém přenosu EHR.

Přístup přijatý při navrhování této dílčí normy musel proto předpokládat, že generické bezpečnostní politiky, komponenty a služby budou přispívat do vyjednávací fáze (*rozhodnutí o přístupu*), která bude předcházet schválení přenosu Extraktu EHR, a že budou chránit aktuální toky dat EHR.

Tato norma proto předpokládá, že je do praxe zavedena celková bezpečnostní politika nebo soubor politik odpovídající ISO/IEC 17799 na všech místech účastnících se přenosu EHR, a předpokládá také, že tyto politiky odpovídají národní a přeshraniční legislativě na ochranu osobních dat splňující ustanovení Směrnice EU 94/95. Mohou být požadovány další politiky vyhovující specifickým národním, místním, odborným nebo organizačním směrnicím použitelným pro přenos nebo použití dat EHR. Definování takových politik je mimo rozsah této normy.

Generická architektura řízení přístupu ke zdravotní péči

Legitimní přístup k datům EHR bude určen širokým rozsahem politik, z nichž některé mohou existovat jako dokumenty, některé budou zakódovány uvnitř aplikací a některé uvnitř komponent formálního systému autorizace. Připouští se, že prodejci a organizace se liší v tom, jak implementují politiky a služby řízení přístupu a rozsah, v jakém jsou v současné době převedeny na počítačový systém.

Norma ISO/TS 22600 Správa privilegií a řízení přístupu (Privilege Management and Access Control (PMAC)), vyvíjená ve WG 4 ISO TC/215, definuje generický logický model pro znázornění privilegií nejvyšší úrovně (entit), politik řízení přístupu, které patří k potenciálním cílovým objektům, a procesu vyjednávání, který je požadován pro dosažení rozhodnutí o přístupu. Norma specifikuje generický přístup k úkolům, například přiřazení rolí entitám a předávání rolí mezi entitami.

Obrázek 2 znázorňuje hlavní pojmy Řízení přístupu založeného na rolích definované v PMAC.

Obrázek 2 – Hlavní pojmy a typy politik definované v Řízení přístupu založeném na rolích

Základní entity (osoby, agenti atd.) jsou přiřazeny k jedné nebo více Funkčním rolím, které budou ovlivněny Strukturálními rolemi, které mají povoleno zastávat. Například osoba, která je lékařsky kvalifikována a je specialistou na dětské nemoci může zastávat jednu nebo více Strukturálních rolí (například konzultant dětského lékaře v nemocnici, vedoucí dětského skríningu pro danou oblast). Tyto Strukturální role jí mohou umožnit čas od času jednat s pacientem ve Funkční roli Osobního klinického lékaře. Funkční role může být trvalá nebo omezená pouze na jedinou uživatelskou relaci. Funkční role jsou mapovány na povolení provést konkrétní úkony (například zápis nových položek do EHR) a na konkrétní objekty (například data EHR, na která má tento držitel role povoleno nahlížet).

Pro účely této normy třída Target_Component (Cílová_Komponenta) znázorněná na obrázku 2 představuje data EHR uchovávaná Poskytovatelem EHR. Třída Target_Policy (Cílová_Politika) obsahuje informace, které definují pravidla pro povolení nebo zamítnutí přístupu k části EHR nebo k celému EHR. Jestliže je EHR_EXTRACT vytvářena a komunikována s těmito daty EHR, relevantní Target_Policies vyžadují také přenos k Příjemci EHR. To vyžaduje interoperabilní zobrazení Target_Policy, která pak může být obsažena v EHR_EXTRACT.

Protože se jednotliví dodavatelé a organizace, aby docílili této infrastruktury, mohou lišit ve vyprojektování a v technologických implementacích, norma PMAC definuje tyto procesy a modely v informačních a výpočetních úrovních pohledu. Jejich specifikace jsou tedy otevřené, nezávislé na platformě, přenosné a škálovatelné, aby podporovaly široký rozsah klinických prostředí a použití v různých zemích, kde mohou být různé národní a odborné předpisy.

Tato dílčí norma předpokládá, že přístup PMAC je logicky použit pro řízení rozhodnutí o přístupu v odezvě na žádost o EHR. Není však jejím předmětem definovat aktuální modely politiky, atributy nebo hodnoty atributů, které jsou potřebné k znázornění jednotlivých případů politiky, nebo způsob, jakým je logický přístup PMAC technicky implementován v jakékoliv organizaci nebo oblasti.

Očekává se, že norma PMAC bude definovat generický (interoperabilní) model politiky pro Cílové politiky, ale tato část normy nebude pravděpodobně zveřejněna dříve než v roce 2006 až 2007. Tato dílčí norma pro bezpečnost přenosu EHR proto zahrnuje informativní model, který může být použit dříve, než bude zmíněná část normy PMAC zveřejněna a přijata širokou veřejností.

Jako doplněk k této vznikající normě navrhuje nová pracovní položka v rámci ISO definovat sady Strukturálních rolí a Funkčních rolí, které mohou být použity mezinárodně k podpoře vyjednávání o politice a překlenování politiky (například během fáze vyjednávání ohledně rozhodnutí o přístupu). Tato norma připouští, že tyto a další normalizované slovníky budou stále více podporovat bohatou interoperabilitu politik přístupu, ale nemohou v tomto stádiu nařídit použití jakéhokoliv speciálně řízeného slovníku, protože žádný neexistuje v normalizované podobě.

Bezpečnostní požadavky specifické pro přenos EHR

Velký počet lékařských, právních a etických požadavků EHR je vyjádřen v ISO/TS 18308, ačkoliv jejich splnění je realizováno zejména prostřednictvím specifických tříd a atributů Referenčního modelu EHR (zveřejněného v části 1 této normy). Následující tabulka uvádí ty požadavky, které se aplikují konkrétněji na tuto dílčí normu.

Tabulka 1 – Seznam požadavků zveřejněných v ISO/TS 18308, které se vztahují na bezpečnost přenosu EHR

COC1.2	EHRA musí podporovat právo na přístup zákazníků k veškerým EHR informacím podléhajícím jurisdikčním omezením.
COC1.3	EHRA musí podporovat zákazníky schopné začlenit informace o vlastní péči, jejich stanovisko k problémům osobní péče o zdraví, úrovně spokojenosti, očekávání a poznámky k tomu, co chtějí zaznamenat do EHRs.
COM2.4	EHRA musí poskytnout auditní záznam procesů výměny, včetně autentizace, aby umožnil identifikaci místa předání a přijetí extraktu EHR. To vyžaduje zodpovědnost za procesy slučování.
PRS1.2	EHRA musí podporovat označování celých EHR a/nebo částí EHR omezených na autorizované uživatele a/nebo záměry. Ty by měly obsahovat omezení na úrovni čtení, zápisu, oprav, ověření a přenosu/zpřístupnění dat nebo záznamů.
PRS1.3	EHRA musí podporovat omezení týkající se soukromí a důvěrnosti na úrovni jak datových sad, tak diskrétních datových atributů.
PRS2.2	EHRA musí podporovat získávání, zaznamenávání a sledování statusu informovaného souhlasu s přístupem k celému EHR a/nebo k jeho částem pro definované záměry.
PRS2.4	EHRA musí podporovat zaznamenávání časových rámců připojených ke každému souhlasu.
PRS3.1	EHRA musí podporovat opatření k definování, připojení, modifikování a odstranění přístupových práv k celému EHR a/nebo k jeho částem.
PRS3.3	EHRA musí podporovat opatření vedoucí k umožnění a omezení přístupu k celému EHR a/nebo k jeho částem v souladu s převažujícím souhlasem a s pravidly přístupu.
PRS3.4	EHRA musí podporovat opatření k oddělenému řízení autorit, doplňujících a /nebo modifikujících EHR a autorit, přistupujících k EHR.
PRS5.1	EHRA musí podporovat zaznamenávání auditního záznamu o přístupu k datům a modifikacích dat v celém EHR nebo jeho částech.
PRS5.2	EHRA musí podporovat zaznamenávání povahy každého přístupu a/nebo modifikace.
STR2.10	EHRA musí vzít v úvahu komplexní ukládání a vyhledávání informací týkajících se péče o pacienta. EHRA musí při nejmenším vzít v úvahu zaznamenávání všech strukturovaných a nestrukturovaných dat o: – [ostatních] – zpřístupněních a souhlasu

Generický model Politiky přístupu k EHR

Při zabývání se těmito požadavky v rámci této normy se připouští, že většina klinických systémů a systémů EHR využívaných v současné době zahrnuje relativně jednoduchá opatření týkající se řízení přístupu, obvykle na podporu potřeb v rámci jednotlivé organizace. Několik z nich je interoperabilních s produkty dodavatele nebo s jinými příslušnými systémy, například s podporou rozhodování, pracovního toku nebo systémů hlášení. Systémy nové generace budou stále více podporovat konfigurovatelné politiky přístupu, které mají být specifikovány, ale k podpoře distribuovaného scénáře EHR budou muset být specifikovány interoperabilně a budou muset být výpočetně interoperabilní. Většina prodejců, zdravotních služeb a sítí lékařské péče pravděpodobně přijme progresivní přístup k obohacení sofistikace politik řízení přístupu, které mohou být podporovány.

Může existovat řada politik vysoké úrovně, které budou řídit zpřístupnění EHR v rámci jakékoliv regionální sítě péče o zdraví. Dnes tyto politiky existují především v papírové podobě nebo jako oprávnění uložená v zakódované podobě v aplikacích a serverech, ale v budoucnu budou reprezentovány jako interoperabilní politiky přístupu v souladu s architekturou PMAC. Některé příklady faktorů, které mohou být v takových politikách specifikovány a vzaty v úvahu při provádění rozhodnutí o přístupu k EHR, jsou uvedeny dále.

Národní, Odborné, Organizační politiky mohou být založeny například na:

a. Charakteristikách uživatele:

jméno a identifikace

povolání, specializace, kvalifikace

funkční role

oddělení nebo klinická specializace, které zastupuje jako jejich člen

organizace, kterou zastupuje jako její člen

b. Charakteristikách přístupu:

datum a čas

místo

fyzické zařízení

síť nebo jiné komunikační mechanismy

mechanismy a rozsah zavedeného šifrování

metoda používané autentizace

c. Organizační politiky mohou také potvrdit oprávnění o:

pacientovi, jehož záznam je právě předmětem přístupu

archetypech, které jsou právě předmětem přístupu

navržené operaci (čtení, zápis, modifikace, komunikace, dotazování atd.)

Pro EHR specifické politiky mohou poskytnout nebo zamítnout souhlas pro:

a. pojmenované/identifikované strany

získat přístup k EHR jako celku

převzít konkrétní funkční nebo strukturální role (například specifikovat zástupce odpovědného za osobní zdravotní péči)

b. specifické klinické prostředí (například oddělení, specializace)
c. specifické funkční role

získat přístup ke konkrétním archetypům

získat přístup ke konkrétním Komponentám záznamu

získat přístup k datům specifické citlivosti

převzít specifické funkce EHR (například čtení, zápis, modifikace, komunikace, dotazování)

d. specifické důvody pro přístup

například přímé poskytování péče, podpora poskytování péče, vyučování, výzkum

požadovaná oprávněnost nebo důkaz (například jestliže musí být poskytnut formální podepsaný souhlas)

Celé spektrum politik přístupu zavedených v organizaci je mimo rozsah této normy, ale tato dílčí norma definuje generickou specifikaci pro zobrazování a komunikování těch částí politik přístupu, které se vztahují přímo k datům v jakémkoliv daném EHR (Cílové politiky). Ty budou často představovat přání pacienta ohledně zpřístupnění dat EHR.

Přenos specifických souhlasů a politik přístupu vyjadřujících přání pacientů nebo jejich zástupců je důležitým aspektem přenosu a interoperability EHR. Takové politiky přispívají k celkovému rozhodnutí o přístupu, učiněnému v odezvě na žádosti o EHR, a je nutné je přenést společně s extrahovanými daty EHR k Příjemci EHR, aby mohl Příjemce tyto politiky použít k řízení jakýchkoliv budoucích přístupů ke stejným datům v rámci své organizace.

Generický model k zobrazení politik souhlasu/přístupu vyjadřujících přání pacienta nebo jiných stran je tedy definovaný v této dílčí normě v kapitole 7. Politiky specifické pro EHR, které musí být zahrnuty v EHR_EXTRACT, mohou být reprezentovány pomocí modelu specifikovaného v této kapitole. Tento model je záměrně rozšiřitelný, aby mohl ošetřit specifikace dalších politik nepředvídaných v době tvorby této normy. Protože se očekává, že budoucí dílčí norma PMAC o bezpečnosti bude definovat interoperabilní model politiky přístupu, který může být použit pro tento účel, je v kapitole 7 také definován model UML, aby umožnil těm, kdo si osvojí tuto normu, aby se řídili jak touto normou, tak normou ISO/TS 22600.

V části 1 normy 13606 Referenční model zahrnuje každá RECORD_COMPONENT v EHR_EXTRACT volitelný atribut Policy_ID, umožňující, aby byly provedeny odkazy na takovéto politiky na jakémkoliv stupni podrobnosti v hierarchii kontejnmentu EHR. Každá RECORD_COMPONENT může tedy odkazovat na jakýkoliv počet politik přístupu nebo prohlášení o souhlasu, která definují zamýšlená nutná privilegia a profily základních entit (uživatelé, agenti, software, zařízení, delegovaní aktéři atd.) pro budoucí přístup k EHR.

Musíme připomenout, že některé politiky se mohou použít na konkrétní RECORD_COMPONENTs v EHR, zatímco další se mohou použít na EHR jako celek.

Politiky přístupu k EHR: minimální specifikace pro interoperabilitu

Informační model v kapitole 7 pro zobrazování a komunikování informací politiky přístupu byl záměrně udržován jako velice generický, aby vzal v úvahu různorodost kriterií politiky, které budou smluvně dohodnuté v různých zemích a regionálních sítích zdravotní péče. V současné době nejsou pro mnoho vhodných charakteristik definovány normalizované slovníky. Model politiky v kapitole 7 je tedy pro interoperabilitu politiky pouze částečnou pomocí.

Mnoho existujících a zděděných systémů by nemuselo být schopno začlenit specifikace bohatě definovaných politik, a mnoho oblastí zdravotní péče by nemuselo být delší dobu schopno takové politiky definovat. Tato dílčí norma tedy definuje jako doplněk k celkovému modelu politiky v kapitole 7 dva slovníky, které mohou poskytnout minimální základ pro provádění rozhodnutí o politice přístupu a zajistit základní úroveň interoperability politiky přístupu, i když na hrubé úrovni.

Tyto dva slovníky jsou:

1. klasifikace citlivosti dat EHR (RECORD_COMPONENTS).
2. klasifikace vyšší úrovně Žadatelů o EHR a Příjemců EHR prostřednictvím sady Funkčních rolí.

Definování citlivosti EHR

V prostředí klinické péče (tj. uvnitř spolupracujících týmů lékařské péče a mezi těmito týmy účastnícími se přímého poskytnutí péče pacientům) je obvyklé otevřeně sdílet informace zdravotního

záznamu. Je jistě přáním obrovské většiny pacientů, aby tyto týmy takové informace otevřeně sdílely, a mnoho pacientů je opravdu překvapeno, jak málo z jejich zdravotního záznamu je dnes sdíleno, když by to tak z důvodu bezpečí a správné kontinuity péče mělo být.

Málo současných systémů zdravotní péče (v papírové podobě nebo elektronicky) definuje komplexní interní sekce řízení přístupu k zdravotním záznamům, které uchovávají. Dokonce, i kdyby bylo považováno za užitečné definovat četné podrobné politiky přístupu, v praxi by mohlo trvat systémům zdravotní péče, národní zdravotnické službě a milionům pacientů docela dlouho zajistit specifikace příslušných politik přístupu pro všechna data EHR a implementovat softwarové komponenty, které mohou provádět mnoho komplexních výpočtů politik přemostění v reálném čase. Udržování těchto politik v závislosti na vývoji požadavků každého pacienta na klinickou péči by mělo být také komplexním procesem.

Zatímco by mohla být teoreticky definována řada politik přístupu (pacienty nebo ostatními), aby poskytla víceúrovňový rámec úrovně přístupu v rámci jakéhokoliv daného EHR, v praxi pracuje většina klinických prostředí na bázi předem určených práv udělených v celém zdravotním záznamu jakémukoliv odborníku na zdravotní péči nebo odborníku v oblasti souvisící se zdravím, který má legitimní zájem o tohoto pacienta. (Definice toho, kdo má takovýto legitimní zájem se mezi organizacemi liší a není předmětem této dílčí normy.) Je však také akceptovatelné, že pacienti a odborníci čas od času potřebují omezit přístup k některým na soukromí citlivějším datům EHR. Ve většině zdravotnických služeb je také obvyklé vyhradit určitým klinickým prostředím výlučné části EHR (například klinikám sexuálního zdraví).

Tento druh vyhrazování účelu klinickým prostředím nebo označování dat EHR jako zvláště citlivá je zcela odlišný od jakýchkoliv dílčích sekcí EHR, které mohou být definovány tak, aby napomohly navigování a pracovnímu toku v klinických specializacích, například definováním části, týkající se rakoviny nebo diabetu v EHR. Obrázek 3 znázorňuje způsob, jakým může být EHR logicky rozdělen z pohledu citlivosti (řízení přístupu).

Klíč

A Privátní položky sdílené s GP	**C Položky přístupné administrativním zaměstnancům**	**E Položky přístupné týmům přímé péče**
B Položky omezené na tým sexuálního zdraví	**D Položky přístupné zaměstnancům klinické podpory**	**F Privátní položky sdílené s několika jmenovitě uvedenými stranami**
G Položky omezené na vězeňské zdravotní služby		

Obrázek 3 – Znázornění přístupových domén v příkladu EHR

Na tomto obrázku se předpokládá, že pacient má úplný přístup ke svému EHR. K většině EHR tohoto pacienta má přístup jakákoliv strana poskytující přímou klinickou péči. EHR však obsahuje několik soukromých položek; některé jsou omezeny na praktického (rodinného) lékaře pacienta a některé na samostatný seznam jmenovitě uvedených stran. EHR také obsahuje některé položky vytvořené klinikou sexuálního zdraví a omezené na tuto kliniku, a další položky omezené na vězeňskou zdravotní službu – k oběma mohou mít přístup pouze strany s příslušným dodatečným privilegiem k této poddoméně. (Pacient však může, jestliže si to přeje, jmenovat další strany s právem přístupu k těmto dílčím souborům EHR s tím, že jim přidělí příslušná privilegia.) Jednou stránkou privilegia je přidělení rolí, které mohou být použity v naléhavém případě, klinickému lékaři, udělující mu práva, která přesahují práva vyplývající z jeho obvyklé role. Takové získání přednosti v naléhavém případě by

mohlo například udělit přístup k širší sadě záznamů pacienta než je to při péči tohoto klinického lékaře běžné. (Takové použití statusu naléhavého případu by vyžadovalo zvláštní záznam a pravidelnou kontrolu.)

K některým částem EHR mají také záměrně přístup zaměstnanci klinické podpory, kteří mohou potřebovat přezkoumat určité klinické nálezy, aby provedli úkoly jako například naplánování vyšetření nebo vyšetření.

K velmi malé části EHR tohoto příkladu mají přístup také správní zaměstnanci. Jmenovaní úředníci, sekretářky a zřízenci potřebují znát určitá důležitá fakta o pacientovi, aby mohli sehrát svoji roli v celkovém poskytnutí účinné péče, například potřebují být obeznámeni s tím, že pacient má speciální zdravotní potřeby, které je třeba prosadit, nebo že bude potřebovat nasadit 24 % kyslík a invalidní vozík, aby mohl být převezen na rentgenologické oddělení.

Tento příklad neukazuje, jakým způsobem mohou být pacienti vyloučeni z přístupu k částem EHR, ale takové dohody mohou být provedeny s použitím rámce generické politiky z kapitoly 7, jestliže to povoluje legislativa na ochranu dat. Příkladem může být důvěrné poskytnutí dat EHR členem rodiny pacienta.

Zatímco sada různorodých politik by mohla být definována pro specifické typy pacientů, pro specifická prostředí nebo jen z toho důvodu, že jeden pacient se zajímá o svůj EHR více než druhý pacient, převzetí distribuovaných řešení EHR vyžaduje, aby bylo řízeno, s přihlédnutím k tomu, že rozumná sada předem určených řešení a jednoduchý systém uspokojí v dohledné době většinu případů. Důvodem je, že sada různorodých politik by nemusela být schopná přímé interpretace a začlenění do systému EHR Příjemce EHR, dokonce i když informace v těchto politikách mohou být komunikovány standardním způsobem.

Tato norma proto kromě generického zobrazení informací o politice přístupu k EHR (Příloha A) definuje také přesný popis minimálního základu pro přenos citlivosti dat EHR v rámci EHR_EXTRACT, specifikací citlivosti RECORD_COMPONENTs, v souladu s klasifikací definovanou v 6.1 této dílčí normy. Tato klasifikace odpovídá různým poddoménám dat EHR znázorněným na obrázku 3.

V praxi by jakýkoliv daný systém EHR mohl mít pro označení citlivosti dat EHR nebo nějakého ekvivalentního pojmu jiné mechanismy. Tato norma nepožaduje, aby systémy EHR uchovávaly data podle stupňů citlivosti definovaných v 6.1, ale požaduje schopnost mapovat na tuto klasifikaci při generování EHR_EXTRACT.

Funkční role pro přístup k datům EHR

Aby mohlo být učiněno rozhodnutí o přístupu, profil a účel zamýšleného Příjemce EHR musí být porovnán s politikami aplikovanými na EHR, které má poskytovatel EHR, včetně citlivosti specifických RECORD_COMPONENTS, které byly požadovány.

Je tedy nutné specifikovat profil žadatele a/nebo příjemce interoperabilním způsobem. Z dřívější diskuse vyplývá, že se požadavky, legislativa, atributy a slovníky použité pro tento účel v každé zemi liší a nemohou být zatím normalizovány.

Aby se však zajistila základní úroveň interoperability, minimální soulad s touto normou požaduje, aby jakákoliv žádost o EHR_EXTRACT zahrnovala jako část specifikace žádosti Funkční roli zamýšleného Příjemce EHR podle definice v 6.2 této dílčí normy.

Tato sada Funkčních rolí je identická se sadou, která má být zahrnuta do pracovní položky ISO DTS 21298 o Funkčních a Strukturálních rolích. Je zde obsažena jako normativní specifikace, protože tato

pracovní položka není v dostatečně pokročilém stavu na to, aby na ni byl v této normě odkaz.

Korelace mezi Funkční rolí a citlivostí EHR pro účely udělení nebo zamítnutí žádosti o přístup nebo pro filtrování EHR_EXTRACT je definována v 6.3 této dílčí normy.

Toto mapování poskytuje základní (na hrubé úrovni) způsob omezení rozsahu přístupu k EHR podle typu strany, která žádá o přístup. V situacích, pro které byla definována interoperabilní specifikace profilu žadatele na místní nebo národní úrovni, může být vždy přidána další sofistikace. Znázornění způsobu, jakým toto základní mapování může být kombinováno s malým počtem dodatečných specifikací pro specifikaci relativně různorodé sady omezení přístupu, je uvedena v kapitole 7.

Interoperabilita Auditního záznamu

Všeobecně se připouští, že podrobnosti interakcí se systémem EHR musí být uchovány pro účely auditu. Avšak způsob, jakým jsou tyto druhy auditních záznamů implementovány, je zcela specifický pro každý systém EHR, částečně určený důsledností (například uchování v databázi) přijatého přístupu, a mohl by být také částečně řízen místní nebo národní legislativou. Formální normy pro interoperabilitu a přenos auditních záznamů nejsou dosud dostupné. Kandidátská specifikace pro zobrazení auditních záznamů byla zveřejněna v roce 2004 jako informační návrh IETF (RFC 3881), ale v současné době neexistuje žádný plán pro formální převzetí tohoto návrhu do IETF jako normy pro interoperabilitu. Protože tato norma EN 13606-4 nespecifikuje model pro úplný přenos informací auditního záznamu, uživatel, který potřebuje interoperabilní specifikaci, může zvážit užitečnost RFC 3881 IETF.

Existuje však stále silnější důkaz, že schopnost pacientů kontrolovat informace o přístupu k jejich datům EHR není jen legitimním právem, ale ve skutečnosti pomáhá podporovat morální chování odborníků na zdravotní péči tím, že přistupují pouze k záznamům, které opravdu potřebují vidět.

Zatímco systémy jednotlivých EHR by mohly být schopny poskytnout určitý stupeň přístupu k auditnímu záznamu, ten je v současnosti obvykle poskytován správcům databáze pomocí nástrojů a rozhraní, které se nehodí pro to, aby umožnily pacientům prohlížet si historii přístupu k jejich vlastnímu EHR. V distribuovaném (sdíleném) scénáři EHR je nutné, aby EHR a záznamy o přístupech k těmto EHR byly také distribuovány.

Interoperabilní specifikace je tedy požadována pro základní sadu dat, které mohou být poskytnuty jako odezva na žádost (pacienta nebo jeho zástupce) o poskytnutí seznamu přístupů k EHR. Toto je proto definováno jako informační model revize auditního záznamu v této dílčí normě (kapitola 8) i jako model rozhraní žádosti a odezvy v části 5 této normy.

Připouští se, že dnes by mohlo jen málo systémů splňovat tento požadavek, takže soulad s tímto ustanovením se posuzuje odděleně od souladu se zbytkem této dílčí normy. Je věcí místní nebo národní politiky určit, zda musí být toto dodatečné ustanovení splněno.

Tento náhled na auditní záznam není míněn jako prostředek, kterým je auditní záznam přezkoumáván jako část formálního vyšetřování přístupů k systému EHR. Tato norma nedefinuje jakékoliv interoperabilní specifikace pro taková posuzování.

Vztah k ENV 13606 Části 3 (Pravidla distribuce)

Pravidla distribuce ENV 13606, zveřejněná v roce 2000, poskytla podrobný analytický rámec pro specifikování požadavků, které musí být splněny, aby mohl být potvrzen přenos dat EHR. Zkušenost současného týmu pracovní skupiny EHR (EHRcom Task force team) je, že tento rámec, ačkoliv je velmi rozmanitý, bylo obtížné implementovat v praxi z několika důvodů:

- některá hlediska specifikace, například Proč (Why) (důvod, pro který byl přenos EHR žádán) jsou definována s textovými atributy bez formalizovaného slovníku, v důsledku čehož je obtížné docílit interoperabilitu;
- celkový rámec byl daleko podrobnější, než prostředky na řízení přístupu většiny současných systémů EHR, a byl by pro implementaci jak nákladný tak obtížný;
- rámec by vyžadoval významné pracovní úsilí od odborníků na zdravotní péči, aby se rozšířily instance pravidel v průběhu vstupu dat EHR;
- mnoho na počítač převedených zdravotních systémů začleňovalo a začleňuje generická bezpečnostní opatření, a přidání specifického přístupu EHR bylo pociťováno jako nadbytečné.

Od roku 2000 vyvinulo mnoho zdravotních služeb strategie na zabezpečení systémů zdravotní péče a komunikací mezi nimi, a mnoho produktů nyní začleňuje generické bezpečnostní komponenty, například certifikační služby a systémy PKI, nebo s nimi mají společné rozhraní. Bezpečnostní normy zveřejněné od roku 2000 se nyní zabývají mnoha aspekty, které bylo proto nezbytné specifikovat v Pravidlech distribuce.

Přístup uplatněný v této dílčí normě má za cíl podporovat použití těchto (generických) bezpečnostních opatření z průmyslových norem nebo z oblasti zdravotnictví, a specifikovat jen ty rysy, které se týkají zvláště přenosu EHR – zejména ustanovení o přístupu, která by mohla být specificky připojená k jakémukoliv danému elektronickému zdravotnímu záznamu. Nejobecnějším příkladem je přání pacienta (datového subjektu) ohledně zpřístupnění.

Podrobnější popis těchto změn je uveden v Příloze B.

1 Předmět normy

Tato část této vícedílné normy o Přenosu elektronických zdravotních záznamů popisuje metodologii pro specifikaci privilegií nezbytných pro přístup k datům EHR. Tato metodologie vytváří část celkové architektury komunikace EHR definované v části 1 této normy.

Tato norma se pokouší řešit ty požadavky, které se jedinečně týkají přenosů EHR a zobrazení a přenosu informací specifických pro EHR, které budou formovat rozhodnutí o přístupu. Odkazuje také na všeobecné bezpečnostní požadavky, které se aplikují na přenosy EHR, a poukazuje na technická řešení a normy, které uvádějí podrobnosti o službách splňujících tyto bezpečnostní potřeby.

POZNÁMKA Bezpečnostní požadavky na systémy EHR nesouvisící s přenosy EHRs jsou mimo rozsah této normy.