internasional jurnal informasi medik i cs 7 6 (2 0 0 7) 449–453

homepage jurnal: www. int l .el sevierheal th. com / jurnal s / i jmi

Model arsip notaris untuk pengamanan dan distribusi dokumen pasien yang ditandatangani secara elektrik

Pekka Ruotsalainen *Sebuah , * ,* ***Bryan Manning*** *b*

Sebuah *Pusat Penelitian dan Pengembangan Nasional untuk Kesejahteraan dan Kesehatan (Pasak) Pusat Keunggulan TIK,*

PO Box 220, 00531 Helsinki, Finlandia

b *Federasi Eropa untuk Informatika Medis, Kelompok Kerja Perencanaan dan Pemodelan Informasi, Pusat Informasi Bisnis, Manajemen Organisasi dan Proses, Westminster Business*

School, University of Westminster, London, Inggris

articleinfo

Kata kunci:

Pengarsipan jangka panjang

Arsip Notaris

Akses data butiran halus

Stempel waktu

Rekor acara

Meta fi le

abstrak

Industri perawatan kesehatan sedang bergerak dari dokumentasi berbasis kertas ke era digital. Catatan kesehatan elektronik (EHR) memainkan peran utama dalam perkembangan ini. Catatan kesehatan elektronik tidak hanya akan dibagikan di antara penyedia layanan kesehatan yang jumlahnya terus bertambah, tetapi juga harus diarsipkan dalam jangka waktu yang lama. Siklus hidup yang diperlukan bergantung pada peraturan nasional, tetapi biasanya waktu penyimpanan data pasien bervariasi antara 20 dan 100 tahun. Ketersediaan, integritas, kerahasiaan, dan non-penolakan data yang disimpan selama periode penyimpanan yang panjang ini perlu dibuktikan sepenuhnya, baik untuk mencegah kehilangan dan juga memastikan kemampuan untuk membaca dan memahami konten dipertahankan.

Dokumen ini menjelaskan arsip notaris terpercaya koperasi (TNA) yang menerima data kesehatan granular dari sistem EHR yang berbeda, menyimpan data bersama-sama dengan informasi pengukuran terkait untuk waktu yang lama dan mendistribusikan objek data EHR granular. TNA berkomunikasi dengan sistem EHR dan pengguna eksternal melalui permintaan arsip dan pesan distribusi. TNA dapat menyimpan objek dalam format XML dan membuktikan non-repudiation dan integritas data yang disimpan dengan bantuan catatan acara, stempel waktu dan arsip tanda tangan elektronik.

1. pengantar

Model-model baru dari pemberian layanan kesehatan menekankan perlunya informasi pasien untuk dibagikan di antara penyedia layanan kesehatan yang jumlahnya terus bertambah bersama dengan pasien itu sendiri. Akibatnya, semakin banyak komunikasi yang terjadi melintasi batas-batas organisasi tradisional. Catatan Electronichealth (EHR) memainkan peran utama dalam perkembangan ini.

Saat data pasien direkam secara elektronik, data tersebut harus disimpan dalam waktu lama baik di database lokal atau di arsip eksternal. Selama beberapa tahun terakhir, berbagai arsip elektronik, seperti PACS — sistem pengarsipan untuk citra medis, telah dibuat, dan tetap independen sistem informasi pasien. Namun, arsip elektronik menjadi layanan penyimpanan informasi inti yang digunakan bersama antara kelompok pengguna yang berbeda. Arsip elektronik ini juga dapat menerima informasi dari berbagai organisasi, dan data yang akan disimpan dapat berisi informasi yang dibuat dalam konteks yang berbeda dan untuk tujuan yang berbeda. [1] .

Biasanya, catatan kesehatan pasien harus ditandatangani setelah episode perawatan oleh dokter yang bertanggung jawab. Dalam lingkungan digital, tanda tangan elektronik juga diperlukan untuk membuktikan integritas dan keaslian data pasien.

Catatan kesehatan elektronik harus diarsipkan dalam jangka waktu yang lama. Siklus hidup yang diperlukan bergantung pada peraturan nasional tetapi biasanya waktu penyimpanan data pasien

* *Penulis yang sesuai.*

Alamat email: pekka.ruotsalainen@stakes. fi (P.Ruotsalainen), bryan.manning@binternet.com (B. Manning). 1386-5056 / $ - lihat materi depan
doi: 10.1016 / j.ijmedinf.2006.09.011

bervariasi antara 20 dan 100 tahun. Ketersediaan, integritas, kerahasiaan, dan non-penolakan data yang disimpan selama seluruh periode penyimpanan harus dibuktikan sepenuhnya [2] .

Penyimpanan data elektronik terancam oleh bahaya dasar yang sama seperti penyimpanan kertas. Data dapat hilang, integritas dapat hilang, bersama dengan kemampuan membaca dan memahami isinya. Masa pakai informasi kesehatan yang disimpan dalam banyak kasus melebihi masa pakai format dan alat teknis yang digunakan untuk menyimpan data. Mungkin juga, bahwa selama periode penyimpanan, validitas beberapa tanda tangan digital mungkin melemah, dan sertifikat PKI mungkin dicabut atau kedaluwarsa. [3] .

Dalam kasus pengawetan catatan kesehatan elektronik jangka panjang, konfirmasi ketersediaan informasi yang disimpan akan menjadi tugas yang berat. Struktur dan format data dapat berubah selama waktu penyimpanan, yang akan mempersulit pencarian dan penggunaan data.

Arsip notaris adalah salah satu solusi yang mungkin, karena memungkinkan ketersediaan dan integritas data yang ditandatangani secara digital untuk dibuktikan bersama dengan mencegah penolakan data yang disimpan selama periode penyimpanan yang lama. Ini sangat penting ketika konversi struktural diperlukan dan data harus ditransfer ke media penyimpanan baru.

2. Definisi

Sebuah *arsip* adalah organisasi yang menyediakan layanan pemeliharaan catatan kesehatan yang memungkinkan akses yang dikontrol secara ketat ke sekelompok konsumen yang teridentifikasi untuk jangka waktu yang diatur [5] . Sebuah *arsip elektronik (* eArchive) mempertahankan format informasi asli. EArchive pasif menyimpan konten data tetap dengan metadata dan kebijakan terkait. Isi data tetap ini harus didefinisikan sepenuhnya dan terstruktur secara atomis dalam aplikasi sebelum dapat dikirim ke arsip. Setelah data diarsipkan, data tidak dapat diubah atau dihapus sebelum waktu penyimpanannya berakhir [4] . Di sisi lain, eArchive aktif memungkinkan akses acak dan pembaruan elemen data apa pun selama waktu penyimpanan.

Sebuah *sistem pengarsipan* adalah sebuah organisasi yang diharuskan untuk menyampaikan informasi yang tersedia dalam bentuk yang benar dan dapat dipahami secara independen selama periode waktu yang ditentukan, dalam batasan akses dan keamanan yang sesuai.

Paket data arsip adalah kumpulan objek data yang diarsipkan dengan informasi terkait, catatan bukti terkait, dan file meta arsip.

Arsip notaris adalah organisasi tepercaya yang menyediakan layanan untuk pelestarian catatan kesehatan jangka panjang dan layanan yang memastikan integritas dan non-penyangkalan data asli dengan memperluas ini untuk menyertakan pembaruan stempel waktu secara berkala dan pengumpulan bukti pendukung. Arsip notaris menjalankan fungsi-fungsi berikut: otentikasi transaksi elektronik, non-repudiation dan konfirmasi integritas data. Setelah arsipotaris memiliki dokumen yang ditandatangani secara elektronik, statusnya sama dengan dokumen yang ditandatangani oleh seseorang [3] .

Sebuah cap waktu itu sendiri adalah pengesahan yang dihasilkan oleh TimestampAuthority bahwa item data tertentu ada dari waktu tertentu [3] .

Arsip cap waktu adalah atribut yang berisi Stempel Waktu dan informasi tambahan yang diperlukan untuk memverifikasi status objek data / grup objek dari waktu yang disertifikasi oleh stempel waktu [3] .

Sebuah catatan bukti adalah kumpulan kumpulan bukti yang terhubung ke satu objek data atau sekelompok objek. Ini dapat mencakup Stempel waktu, data verifikasi, sertifikat PKI dan informasi kebijakan keamanan. Ini dapat digunakan untuk menjaga informasi deskriptif sehingga kepercayaan dapat dibangun pada sertifikat setelah mereka kedaluwarsa. Catatan bukti harus ditandatangani sedemikian rupa sehingga setiap modifikasi objek data atau catatan bukti dapat dideteksi [3] .

Aturan adalah kumpulan aturan yang menjelaskan tindakan mana yang diperbolehkan dalam keadaan tertentu. Kebijakan keamanan dan kebijakan pengarsipan adalah kebijakan dasar yang diperlukan untuk pelaksanaan arsip apa pun.

3. Persyaratan untuk pengarsipan yang aman dari catatan kesehatan

Peran utama dari sistem pengarsipan adalah membuat informasi tersedia dalam bentuk yang benar dan dapat dipahami secara independen selama seluruh periode penyimpanan yang diatur. Itu juga harus menjamin ketersediaan jangka panjang, integritas dan kerahasiaan dari semua data yang disimpan selama periode ini. Pengarsipan digital catatan kesehatan juga harus memenuhi persyaratan peraturan yang ditetapkan oleh undang-undang, misalnya waktu penyimpanan yang ditetapkan oleh undang-undang nasional [4] .

Layanan eArchive juga memiliki tanggung jawab [5] untuk:

- mengelola perubahan dalam status hukum EHR selama waktu penyimpanan;
- mengelola kondisi akses utama;
- mengelola persetujuan pasien;
- melindungi data EHR berdasarkan tujuan dan konteksnya;
- membuktikan keaslian data EHR yang disimpan.

Agar informasi yang disimpan dapat diakses dan dipahami oleh mereka yang membutuhkan akses, data transaksional terkait dan data historis terkait lainnya yang dikumpulkan selama periode penyimpanan harus disimpan bersama dengannya. Data ini terdiri dari informasi deskripsi deskriptif, representasi, isi dan pelestarian yang harus diarsipkan bersama dengan data aktual sebagai satu kesatuan informasi. Arsip juga harus mengatur migrasi data atau terjemahan selama waktu penyimpanan [6] .

4. Persyaratan keamanan yang terpercaya arsip notaris

Arsip catatan tepercaya (TNA) menyimpan catatan kesehatan yang ditandatangani untuk waktu yang lama dan harus memenuhi persyaratan keamanan umum yang ditetapkan dalam Bagian 3 atas. Tugas keamanan tambahan TNA adalah untuk membuktikan integritas dan asal data serta untuk membuktikan non-repudiation data selama seluruh periode preservasi. Integritas harus dibuktikan setelah migrasi data, yang membutuhkan perubahan format. TNA juga harus mencakup layanan untuk memverifikasi tanda tangan dan integritas data, serta membuktikan bahwa peristiwa tertentu telah terjadi.

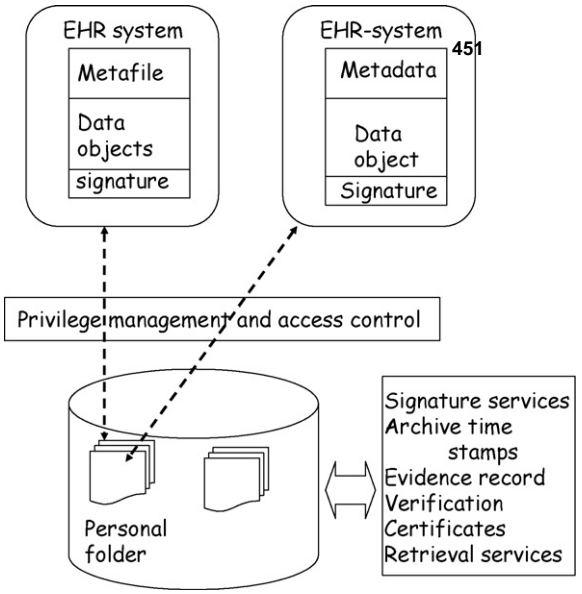
Untuk memenuhi persyaratan tersebut, TNA harus:

- mengumpulkan bukti;
- membuat catatan bukti;
- menghasilkan dan memperbarui arsip Perangko waktu;
- dokumen tanda tangan elektronik;
- membuat log audit

dan kemudian menyimpan informasi ini dengan andal selama seluruh periode pengarsipan [3] .

5. Model arsip notaris untuk pelestarian dan distribusi catatan kesehatan digital

Ada kombinasi yang berbeda dari sistem dan arsip EHR. Sistem pengarsipan elektronik dapat diklasifikasikan sebagai terpusat, kooperatif atau federasi. EArchive terpusat dapat dianggap sebagai bagian tertanam dari sistem EHR perusahaan. Dalam hal ini, sistem EHR dan arsip memiliki kebijakan keamanan terpusat yang sama, kontrol akses dan layanan manajemen hak istimewa.



Gbr. 1 - Sistem TNA dan EHR kooperatif.

Arsip dan sistem EHR juga dapat membentuk sistem informasi koperasi. Dalam hal ini, eArchive berkomunikasi dengan sistem EHR biasanya dalam bentuk permintaan dan jawaban data. Sistem EHR mengirimkan data ke arsip dan menerima data darinya. Contoh tipikal dari kombinasi semacam ini adalah PACS yang berkomunikasi dengan sistem EHR menggunakan DICOMmessages.

EArchive federasi adalah perluasan dari pendekatan koperasi yang melibatkan sejumlah organisasi terpisah dan sering kali tersebar luas, yang menggabungkan sumber daya mereka sebagai "Perusahaan Virtual" [7] dan beroperasi dalam perjanjian pihak ketiga tepercaya [8,9] .

Akibatnya, sistem EHR dan arsip itu sendiri membentuk sistem terdistribusi dengan berbagai kompleksitas bergantung pada jumlah pihak yang terlibat. Meskipun hal ini memerlukan manajemen layanan yang ketat secara keseluruhan, hal ini memiliki keuntungan dalam memberikan ketahanan yang lebih besar dan kemampuan kelangsungan bisnis dalam menghadapi potensi risiko operasional atau intervensi jahat.

Model eArchive untuk melestarikan catatan kesehatan digital dijelaskan di sini dan diilustrasikan di Gambar 1 menguraikan pendekatan kerja sama yang melekat dalam arsip notaris tepercaya (TNA), yang mungkin berkomunikasi dengan berbagai sistem EHR yang berbeda, di tingkat lokal, regional dan nasional. Sementara satu eArchive ditampilkan untuk kesederhanaan, baik ukuran potensinya serta persyaratan cadangan dan pemulihan bencana menentukan bahwa pada kenyataannya ini akan menjadi fasilitas penyimpanan data berbasis multi-situs yang saling berhubungan dan kompleks.

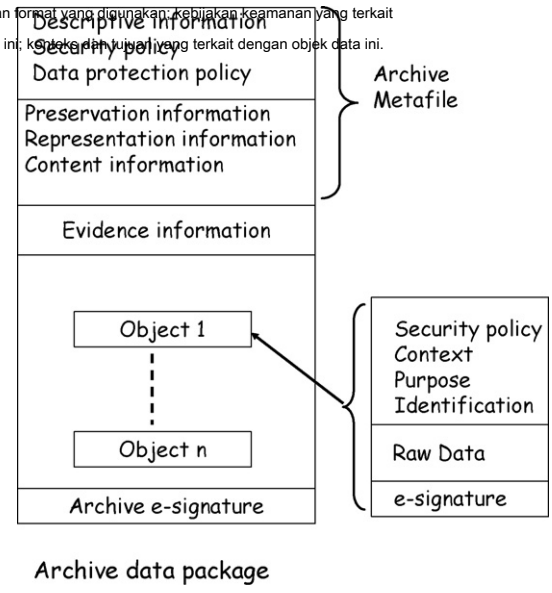
TNA mendukung pengumpulan data multi-sumber. Ini menyimpan objek tunggal bertanda tangan (EHR) atau dokumen yang memiliki struktur data multigrain (misalnya kelompok objek) yang diterima dari sistem EHR yang berbeda untuk periode yang ditentukan dalam meta fi le yang terkait dengan objek data.

TNA mengumpulkan objek data yang memiliki kode identifikasi yang sama (misalnya objek milik pasien yang sama) dan menyimpannya dalam satu folder pasien virtual. TNA memiliki layanan manajemen catatan bukti untuk membuktikan non-penolakan objek dan layanan log audit yang aman. TNA juga punya sistem manajemen tanda tangan untuk menghasilkan Stempel Waktu arsip dan tanda tangan elektronik arsip.

Gambar 2 menunjukkan model data konseptual yang digunakan baik dalam komunikasi antara sistem EHR dan TNA dan untuk pelestarian jangka panjang. Setiap objek data yang menyimpan data mentah juga menyertakan file definisi (file meta).

File ini terdiri dari informasi berikut:

- kode identifikasi peserta (misalnya dari sistem EHR dan pasien);
- kebijakan arsip di mana objek yang diserahkan harus ditangani termasuk waktu penyimpanan data;
- klasifikasi, kode dan format yang digunakan; kebijakan keamanan yang terkait
- dengan objek data ini; konteks dan tujuan yang terkait dengan objek data ini.
-



Gambar 2 - Model paket data arsip.

Dalam model ini, file deskripsi disertakan dalam konten setiap objek data. File ini mencakup juga informasi tentang bagaimana objek yang berbeda dari grup objek dikaitkan satu sama lain.

Sebelum mengirim objek data ke TNA untuk disimpan, sistem EHR (pengirim data) harus:

- mengumpulkan objek data;
- hitung kode identifikasi kontainer (misalnya kode hash);
- tulislah file deskripsi objek yang terkait dengan objek data tersebut;
- menempatkan semuanya menjadi satu wadah data.

Setelah tahapan yang dijelaskan di atas telah diselesaikan, sistem EHR harus menandatangani seluruh penampung [3] . Setelah selesai, sistem EHR kemudian mengirimkan kontainer ke TNA sebagai bagian dari pesan permintaan pengarsipan.

5.1. Proses pengarsipan dasar

Sebelum pemeliharaan teknis, TNA menerima pesan permintaan pengarsipan, yang mencakup wadah data, dan mengubah objek data dan file definisi terkait menjadi paket data arsip. Langkah selanjutnya adalah membangun meta fi le pengarsipan untuk objek yang diterima. File ini merupakan kombinasi dari kebijakan pengarsipan, preservasi, representasi data dan informasi konten data [2,6] . TNA juga mengumpulkan peristiwa, menghasilkan arsip-Cap-waktu, merumuskan catatan bukti, dan menyimpan objek, meta fi le dan catatan bukti ke dalam paket arsip dan akhirnya menandatangani paket itu. [3] . Paket data arsip dapat disimpan dalam format XML [10] .

Selama periode pelestarian, TNA perlu memperbarui pengarsipan Stempel waktu secara berkala untuk membuktikan tidak adanya penyangkalan data. [3] . TNA juga harus mengelola log audit yang aman, yang mencakup informasi semua peristiwa yang terkait dengan aktivitas penyimpanan dan pengungkapan data. Anda juga perlu mengirim pemberitahuan ke sistem EHR untuk memastikan bahwa data yang benar telah diterima untuk pengawetan.

5.2. Distribusi data yang aman

TNA dapat mendistribusikan objek data tunggal dan kelompok objek data. Objek akan didistribusikan dalam paket distribusi data. Paket semacam itu mirip dengan paket data anarsip; namun TNA harus menambahkan informasi identifikasi arsip dan Stempel waktu ke paket ini untuk memastikan waktu distribusi. Mekanisme distribusi data butiran halus ini memungkinkan untuk mengumpulkan objek data yang dikirim oleh sumber berbeda dan mendistribusikannya pada waktu yang sama.

Untuk distribusi data, TNAmemiliki dua model layanan dasar. Model pertama digunakan di mana sistem EHR mengakses objek data yang telah dikirim sebelumnya ke TNA (yaitu sistem EHR mencoba untuk mendapatkan kembali objek yang telah dikirim sebelumnya). Model kedua digunakan dalam kasus di mana pengguna eksternal mencoba mengakses objek data yang disimpan atas nama sistem EHR lain.

Dalam kasus pertama, TNA dan sistem EHR harus memiliki tingkat kebijakan keamanan yang sama. Dalam kasus ini, sistem EHR menggunakan data yang diterima dari TNA dengan cara yang sama seperti menggunakan data lokalnya sendiri dan tidak perlu meminta persetujuan pasien untuk akses data. Untuk memulai transmisi data, file EHR-systems mengirimkan permintaan distribusi data ke TNA. Pesan ini mencakup identifikasi sistem EHR dan informasi yang diperlukan untuk pengambilan objek data yang diperlukan. Saat menerima, TNA mengumpulkan salinan yang diperlukan dari objek data dan mengembalikannya ke sistem EHR untuk digunakan lebih lanjut.

Dalam kasus kedua, pengguna atau proses eksternal mencoba mengakses objek data yang disimpan di TNA. Dalam hal ini, diperlukan pengelolaan hak istimewa dan mekanisme kontrol akses yang lebih terperinci. Setelah pengidentifikasi pemohon, TNA pertama-tama harus memeriksa kebijakan keamanan pemohon. Langkah selanjutnya adalah menganalisis pesan permintaan akses untuk memastikan bahwa pesan tersebut berisi semua informasi yang diperlukan TNA untuk mengizinkan atau menolak akses data. Pesan permintaan akses harus berisi informasi berikut [11] :

- identifikasi pasien;
- identifikasi pemohon data dan peran fungsional dan strukturalnya;
- tujuan dan konteks di mana data akan digunakan; objek data atau kategori objek mana yang
- akan diakses;
- persetujuan pasien.

Untuk mengizinkan akses data untuk setiap pengguna eksternal, TNA harus memiliki manajemen hak istimewa dan layanan kontrol akses yang mampu membuat keputusan tentang kebijakan keamanan, tujuan dan konteks data, peran, persetujuan dan akses berbasis aturan [12,13] . Aturan akses juga harus mencakup kondisi khusus di mana kondisi akses yang disebutkan di atas dapat ditolak (misalnya di mana akses diizinkan oleh undang-undang).

5.3. Pengiriman data parsial

TNA dapat mendistribusikan objek data tunggal atau kumpulan objek data. Sayangnya, banyak EHR saat ini tidak memiliki struktur data granular yang terdefinisi dengan baik dan mereka hanya dapat mengirim seluruh EHR sebagai objek tunggal ke TNA. Pengiriman parsial terjadi dalam situasi di mana pengguna data ingin mengakses hanya beberapa bagian dari EHR, yang telah disimpan sebagai objek tunggal. Untuk memungkinkan akses data dalam situasi seperti ini, TNA harus menyertakan kemampuan layanan pengiriman parsial.

Dalam kasus pengiriman parsial, TNA harus mengumpulkan item data yang diminta dari EHR yang diarsipkan dan mengubahnya menjadi objek data baru. TNA juga harus menulis file meta untuk objek baru ini dan menambahkan tag "Pengiriman sebagian" padanya. Langkah selanjutnya adalah membuat catatan bukti untuk dikaitkan dengan objek data baru dan menambahkan cap waktu. Akhirnya, TNA harus meletakkan semua informasi ini ke dalam wadah data, menandatanganinya menggunakan tanda tangan arsip dan mengirim wadah tersebut ke pengguna.

TNA juga harus mengarsipkan semua objek data parsial terdistribusi yang memiliki tag "Pengiriman sebagian" ke dalam sub arsip terpisah. Objek data ini harus memiliki periode penyimpanan yang sama yang ditetapkan sebagai EHR asli tempat mereka diekstraksi.

5.4. Proses pemutakhiran data di TNA

Sistem EHR menggunakan objek data yang diambil dari TNA untuk tujuan klinis atau hukum lainnya. Selama perawatan pasien

episode, beberapa objek dimodifikasi dan objek baru juga akan dibuat. Setelah akhir episode perawatan, EHR pasien akan diperbarui dengan objek data yang dimodifikasi dan baru, dan EHR yang diperbarui akan dikirim ke TNA. Dari sudut pandang TNA, EHR terlihat seperti dokumen dinamis

[14] .

Dalam kasus ini, TNA menerima catatan pasien yang diperbarui dan menandainya sebagai versi terbaru. Versi terbaru ini akan ditandatangani dan disimpan oleh arsip. Versi terbaru digunakan untuk tujuan distribusi data di masa mendatang dan versi yang lebih lama disimpan ke dalam arsip riwayat untuk keperluan verifikasi. Manfaat dari metode ini adalah bahwa TNA hanya dapat mengelola cascading signature, bukan bersarang.

6. Diskusi

Pengarsipan informasi kesehatan pribadi jangka panjang yang aman dalam format digital merupakan masalah penting yang perlu diselesaikan selama beberapa tahun ke depan. Dua masalah utama yang harus diselesaikan adalah:

- bagaimana mengarsipkan non-repudiation data yang diarsipkan;
- bagaimana membuktikan integritas informasi yang disimpan setelah migrasi digital.

Arsip Notaris Terpercaya (TNA) merupakan jawaban yang menjanjikan atas permasalahan tersebut.

Model TNA yang dijelaskan dalam makalah ini ditargetkan untuk menerima data EHR granular dari sistem EHR yang berbeda; menyimpan objek data untuk waktu yang lama dan mendistribusikannya seperti yang diminta secara sah. TNA berkomunikasi dengan sistem EHR dan pengguna eksternal melalui permintaan arsip dan pesan distribusi. TNA dapat menyimpan objek data dalam format XML dan membuktikan validitas setiap peristiwa yang telah terjadi selama periode penyimpanan yang diatur. Model TNA ini juga memiliki keuntungan tambahan yaitu hanya kunci yang digunakan oleh TNA yang harus disimpan untuk periode ini. Akibatnya, tidak perlu menyimpan kunci tanda tangan pribadi profesional perawatan kesehatan

[3] .

Seperti yang dijelaskan dalam model TNA, informasi kesehatan pasien yang diterima dari berbagai sumber disimpan dalam satu folder data pribadi, yang di masa mendatang dapat membentuk catatan kesehatan pribadi seumur hidup pasien.

Dalam jangka panjang, komunikasi yang hanya didasarkan pada jenis pesan ini tidak akan cukup. Di masa depan, perawatan tanpa batas lintas organisasi, profesional kesehatan keliling, dan pasien akan memerlukan akses dinamis ke data granular. Ini dapat difasilitasi oleh perluasan model TNA ini di masa depan; namun, ini akan membutuhkan mekanisme distribusi hak istimewa yang dinamis yang harus dikembangkan [15] .

Kemampuan untuk menyimpan objek data yang mungkin memiliki tujuan, konteks, dan kebijakan keamanan yang berbeda memungkinkan tidak hanya untuk menyimpan catatan kesehatan resmi, tetapi juga informasi lain, seperti dokumen atau data yang dibuat dan dimiliki oleh pasien sendiri (misalnya pengukuran rumah dan laporan pemantauan status kesehatan).

referensi

[1] P. Ruotsalainen, Persyaratan Keamanan dalam EHR-sistem dan Arsip, Perawatan Medis dan Kompunetik 1, Studi di Teknologi Kesehatan dan Informatika, vol. 103, IOS Press, 2004, hlm. 453–458.

[2] P. Ruotsalainen, Mengarsipkan data: bagaimana melakukannya? Siapa yang bisa mengakses? Tutorial SP6, dalam: Konferensi dan Pameran TI Kesehatan Eropa Tahunan Keenam (TEHRE 2001), 11-14 November, 2001.

[3] L.Wallace, Layanan Arsip dan Notaris Jangka Panjang, LTANS, LTAP, IETF (www.ietf.org/internet-drafts/drafts-ietf-ltans). Strategi Pengarsipan Digital untuk Kepatuhan Peraturan dalam Perawatan Kesehatan,

[4] Buku Putih, Archiva, Inc. (www.archivas.com). ISO / TC 215, Informatika Kesehatan — Persyaratan Keamanan untuk Pengarsipan Catatan Kesehatan Elektronik, Prinsip dan

[5] Persyaratan ISO / PDTS part1, 15-09-2006.

[6] Consultative Committee for Space Data Systems (CCDS), Reference Model for Open Archival Information System (OAIS), RED BOOK, Washington, DC, USA, Juni 2001.

[7] M. McKeon Stosuy, B. Manning, "Bergabung" Layanan e-Health dan e-Care, Perawatan Medis dan Kompunetik 2, Studi di Teknologi Kesehatan dan Informatika, vol. 114, IOS Press, 2005, hlm. 65–81.

[8] Itu *tScheme* Panduan Pengamanan Transaksi Elektronik, *tScheme* Ltd., September 2002 (www.tScheme.org). Manajemen Pihak Ketiga

[9] Tepercaya: *tScheme* dan Keyakinan dalam Identitas Online, *tScheme* Ltd., September 2004 (www.tScheme.org).

[10] H.Peterson, penyimpanan jangka panjang informasi perawatan kesehatan elektronik dalam format XML, The PARK Project, Swedia, 2000.

[11] E. Coiera, R. Clarge, e-Consent: desain dan implementasi mekanisme persetujuan konsumen dalam lingkungan elektronik, J. Am. Med. Assoc. 11 (Maret / April (2)) (2004).

[12] B. Blobel, Analisis, desain dan implementasi sistem informasi kesehatan terdistribusi yang aman dan dapat dioperasikan. Studi Teknologi Kesehatan dan Informatika, vol. 89, IOS Press, 2002.

[13] Bahasa Otorisasi Privasi Perusahaan (EPAL 1.1), Laporan Riset IBM, IBM 2000–2003.

[14] R. Ruusalepp, RIKSARKIVET, pelestarian digital dalam arsip: gambaran umum penelitian dan praktik terkini, Estonian Business Arch. (2005).

[15] JM Gardier, Identity federation - pengenalan, nilai dan evaluasi, ISSE 2005 - mengamankan proses bisnis elektronik, dalam: Highlights of the Information Security Solution Europe 2005 Conference, Vierweg, 2005.