INSO
20618
1st.Edition
2016

جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان ملی استاندارد ایران
Iranian National Standardization Organization

استاندارد ملی ایران
۲۰۶۱۸
چاپ اول
۱۳۹۴

داده‌ورزی سلامت – روندهای ممیزی برای سوابق الکترونیکی سلامت

Health informatics — Audit trails for electronic health records

ICS:35.240.80

سازمان ملی استاندارد ایران

تهران، ضلع جنوب غربی میدان ونک، خیابان ولیعصر، پلاک ۲۵۹۲

صندوق‌پستی: ۶۱۳۹-۱۴۱۵۵ تهران- ایران

تلفن: ۵-۸۸۸۷۹۴۶۱

دورنگار: ۸۸۸۸۷۰۸۰ و ۸۸۸۸۷۱۰۳

کرج ، شهر صنعتی، میدان استاندارد

صندوق پستی: ۱۶۳-۳۱۵۸۵ کرج - ایران

تلفن: ۸- ۳۲۸۰۶۰۳۱ (۰۲۶)

دورنگار: ۳۲۸۰۸۱۱۴ (۰۲۶)

رایانامه: standard@isiri.org.ir

وبگاه: http://www.isiri.org

Iranian National Standardization Organization (INSO)

No.1294 Valiasr Ave., South western corner of Vanak Sq., Tehran, Iran

P. O. Box: 14155-6139, Tehran, Iran

Tel: + 98 (21) 88879461-5

Fax: + 98 (21) 88887080, 88887103

Standard Square, Karaj, Iran

P.O. Box: 31585-163, Karaj, Iran

Tel: + 98 (26) 32806031-8

Fax: + 98 (26) 32808114

Email: standard@isiri.org.ir

Website: http://www.isiri.org

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

سازمان ملی استاندارد ایران به موجب بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفهٔ تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

تدوین استاندارد در حوزه‌های مختلف در کمیسیون‌های فنی مرکب از کارشناسان سازمان، صاحب‌نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود و کوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و واردکنندگان، مراکز علمی و تخصصی، نهادها، سازمان‌های دولتی و غیردولتی حاصل می‌شود. پیش‌نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی‌نفع و اعضای کمیسیون‌های مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔملی مرتبط با آن رشته طرح و در صورت تصویب، به‌عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می‌شود.

پیش‌نویس استانداردهایی که مؤسسات و سازمان‌های علاقه‌مند و ذی‌صلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند درکمیته ملی طرح، بررسی و درصورت تصویب، به عنوان استانداردملی ایران چاپ و منتشر می‌شود. بدین ترتیب، استانداردهایی ملی تلقی می‌شود که بر اساس مقررات استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔملی استاندارد مربوط که در سازمان ملی استاندارد ایران تشکیل می‌شود به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین‌المللی استاندارد ((ISO[1]،کمیسیون بین‌المللی الکتروتکنیک (IEC)[2] و سازمان بین‌المللی اندازه‌شناسی قانونی(OIML)[3] است و به‌عنوان تنها رابط[4] کمیسیون کدکس غذایی(CAC)[5] در کشور فعالیت می‌کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی‌های خاص کشور، از آخرین پیشرفت‌های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود.

سازمان ملی استاندارد ایران می‌تواند با رعایت موازین پیش‌بینی شده در قانون، برای حمایت از مصرف‌کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست‌محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری کند. سازمان می‌تواند به منظور حفظ بازارهای بین‌المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری کند. همچنین برای اطمینان بخشیدن به استفاده‌کنندگان از خدمات سازمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه‌ها و مراکز واسنجی (کالیبراسیون) وسایل سنجش، سازمان ملی استاندارد این‌گونه سازمان‌ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن‌ها اعطا و بر عملکرد آن‌ها نظارت می‌کند. ترویج دستگاه بین‌المللی یکاها، واسنجی وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

1- International Organization for Standardization
2- International Electrotechnical Commission
3- International Organization for Legal Metrology (Organisation Internationale de Metrologie Legals)
4-Contact point
5- Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

«داده‌ورزی سلامت – روندهای ممیزی برای سوابق الکترونیکی سلامت»

رئیس:	**سمت و/یا محل اشتغال:**
حسینی سنو، سیدامین (دکترای کامپیوتر، شبکه‌های کامپیوتری)	رئیس مرکز آموزش‌های مجازی دانشگاه فردوسی مشهد
دبیر:	
مهرشاد، بتول (فوق‌لیسانس MBE)	مدیرعامل شرکت طراحان مبتکر کسری-دانشجوی دکترای مدیریت فناوری اطلاعات دانشگاه فردوسی مشهد
اعضا: (اسامی به ترتیب حروف الفبا)	
آذرکار، علی (فوق‌لیسانس مهندسی نرم‌افزار)	نماینده سازمان نظام صنفی رایانه‌ای کشور
احسان‌بخش، علیرضا (پزشک متخصص رادیولوژی)	عضو هیئت‌علمی دانشگاه علوم پزشکی بیرجند
جودی، الهام (فوق‌لیسانس مدیریت فناوری اطلاعات)	کارشناس- دانشجوی دکترای مدیریت فناوری اطلاعات دانشگاه فردوسی مشهد
دوست‌محمدی، وحید (فوق‌لیسانس صنایع گرایش فناوری اطلاعاتی)	کارشناس مرکز مدیریت راهبردی افتا
عروجی، سیدمهدی (فوق‌لیسانس مدیریت فناوری اطلاعات)	کارشناس سازمان تنظیم مقررات
مالکی، مهدی (فوق‌لیسانس مدیریت دولتی)	معاون اداره کل استاندارد خراسان جنوبی
مهرشاد، ناصر (دکترای مهندسی پزشکی - بیوالکتریک)	رئیس دانشگاه صنعتی بیرجند
مهرشاد، ملیحه (دکترای میکروبیولوژی - بیوانفورماتیک)	شرکت طراحان مبتکر کسری

فهرست مندرجات

پیش‌گفتار

استاندارد «داده‌ورزی سلامت – روندهای ممیزی برای سوابق الکترونیکی سلامت» که پیش‌نویس آن در کمیسیون‌های مربوط تهیه و تدوین شده است، در یکصدوهشتادوششمین اجلاسیه کمیتهٔ ملی مدیریت کیفیت مورخ ۱۳۹۴/۱۲/۱۶ تصویب شد. اینک این استاندارد به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

استانداردهای ملی ایران بر اساس استاندارد ملی ایران شمارهٔ ۵ (استانداردهای ملی ایران- ساختار و شیوهٔ نگارش) تدوین می‌شوند. برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینهٔ صنایع، علوم و خدمات، استانداردهای ملی ایران در صورت لزوم تجدیدنظر خواهند شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدیدنظر در کمیسیون‌های مربوط موردتوجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی ایران استفاده کرد.

منبع و مأخذی که برای تهیه و تدوین این استاندارد مورد استفاده قرار گرفته به شرح زیر است:

ISO 27789:2013(E), Health informatics — Audit trails for electronic health records

مقدمه

۰-۱ کلیات

اطلاعات شخصی بهداشت و سلامت از نظر بسیاری افراد به‌عنوان محرمانه‌ترین انواع اطلاعات شخصی در نظر گرفته می‌شود و حفاظت از محرمانگی آن برای حفاظت از فضای شخصی افراد تحت مراقبت بسیار ضروری است. به‌منظور تأمین یکپارچگی داده‌ورزی بهداشت و سلامت بسیار مهم است که تمام چرخه عمر این اطلاعات به‌طور کامل قابل ممیزی باشد. سوابق سلامت[1] باید به نحوی ایجاد، پردازش و مدیریت شود که تضمین‌کنندهٔ یکپارچگی و محرمانگی محتویات بوده و امکان کنترل قانونی بر نحوه ایجاد، استفاده و نگهداری سوابق را برای افراد تحت مراقبت تأمین کند.

اطمینان به سوابق الکترونیکی سلامت نیاز به عناصر امنیتی فنی و فیزیکی و همچنین عنصر یکپارچگی داده دارد. از میان مهمترین نیازمندی‌های امنیتی برای حفاظت از اطلاعات شخصی بهداشت و سلامت و یکپارچگی سوابق می‌توان به موارد مرتبط با ممیزی[2] و واقعه‌نگاری[3] اشاره کرد. این مسئله امکان پاسخگویی به افراد تحت مراقبت که اطلاعات سلامت و بهداشت خود را در اختیار سامانه‌های سوابق الکترونیک بهداشت و سلامت (EHR)[4] قرار داده‌اند را فراهم می‌کند. این موارد همچنین به حفظ یکپارچگی سوابق نیز از طریق تأمین انگیزه مشترک قوی بین کاربران این سامانه‌ها برای هماهنگی با سیاست‌های سازمانی در راستای کاربرد این سامانه‌ها، کمک می‌کند.

ممیزی و واقعه‌نگاری مؤثر می‌تواند به کشف سوءاستفاده از سامانه‌های EHR یا داده EHR کمک کند. به‌علاوه، این امر می‌تواند به سازمان‌ها و افراد تحت مراقبت نیز برای دریافت خسارت از کاربرانی که از حقوق و امتیاز انحصاری خود سوءاستفاده می‌کنند؛ کمک کند؛ بنابراین به‌منظور انجام دقیق فرآیند ممیزی ضروری است که روند ممیزی[5] میزان مناسبی از اطلاعات کارآمد را در برگیرد تا بتواند شامل محدوده وسیعی از رخدادها شود (پیوست الف را مشاهده کنید).

واقعه‌نگاری از سیاههٔ[6] ممیزی به‌عنوان مکمل برای کنترل دسترسی در نظر گرفته می‌شود. سیاهه‌های ممیزی همچنین ابزاری را برای ارزیابی جلب رضایت کاربر و اعمال سیاست دسترسی سازمانی به اطلاعات فراهم می‌کند و می‌تواند در ارتقاء و بهینه‌سازی سیاست‌های موجود نیز مؤثر باشد؛ اما ازآنجاکه چنین سیاستی باید امکان پیش‌بینی وقوع موارد پیش‌بینی‌نشده یا ضروری را داشته باشد، لذا تحلیل سیاهه‌های ممیزی ابزارهای اولیه تأمین دسترسی به اطلاعات و موارد مذکور است.

---

1 - Health records
2 - Audit
3 -Logging
4 - Electronic Health Record
5 - Audit trail
6 -Log

این استاندارد ملی به‌طور اختصاصی به محدودهٔ واقعه‌نگاریِ رویدادها می‌پردازد. فرض می‌شود تغییرات مقادیر داده در فیلد[1]های EHR، در خودِ سامانه پایگاه داده EHR ثبت می‌شوند و نه در بخش سیاههٔ ممیزی. فرض می‌شود که خود سامانهٔ EHR حاوی مقادیر قبلی و به‌روز شده در تمامی فیلدها است. این امر با ساختار پایگاه‌های داده یک نقطه در زمان[2] نیز سازگار است. سیاههٔ ممیزی شامل هیچ‌گونه اطلاعات شخصی بهداشت و سلامت نیست و تنها شامل شناسه‌ها و پیوندهایی به سوابق موردنظر است.

سوابق الکترونیک بهداشت و سلامت حاوی اطلاعات شخصی فرد است و ممکن است در سامانه‌های اطلاعاتی مختلفی در داخل و در محدوده‌های سازمانی و یا حتی قضایی قرار داشته باشد. به‌منظور آگاهی از روند کلیه اقدامات انجام‌شده بر روی سوابق یک فرد تحت مراقبت، وجود یک چارچوب مشترک یک پیش‌نیاز است. این استاندارد ملی چنین چارچوبی را ارائه می‌دهد. به‌منظور پشتیبانی از روند ممیزی در بین دامنه‌های مجزا، ارجاع به این چارچوب برای سیاست‌هایی که نیازمندی‌ها را در این دامنه مشخص می‌کنند، از قبیل قوانین کنترل دسترسی و دورهٔ نگهداری، ضروری است. سیاست‌های دامنه می‌توانند به‌صورت تلویحی از طریق شناسایی منابع سیاههٔ ممیزی مرجع‌دهی شوند.

۰-۲ مزایای استفاده از این استاندارد ملی

استانداردسازی روند ممیزی در دسترسی‌ها به سوابق الکترونیکی بهداشت و سلامت دو هدف کلی دارد:

- تضمین اینکه اطلاعات ثبت‌شده در سیاههٔ ممیزی به‌منظور شبیه‌سازی دقیق ترتیب زمانی وقوع وقایعی که تشکیل‌دهنده محتوای سابقهٔ الکترونیک بهداشت و سلامت هستند کارآمد هستند.

- تضمین اینکه روند ممیزی اقدامات انجام‌شده برای سوابق یک فرد تحت مراقبت به‌راحتی قابل‌اجرا و پیگیری است حتی در بین دامنه‌های سازمانی.

این استاندارد ملی برای افراد مسئول نظارت بر امنیت و محرمانگی اطلاعات بهداشت و سلامت و برای سازمان‌های بهداشت و درمان و سایر متولیان اطلاعات بهداشت و سلامت که نیازمند دستورالعمل در زمینه ممیزی سلامت هستند و همچنین رایزنان امنیتی، مشاوران، ممیزان، توزیع‌کنندگان و ارائه‌دهندگان خدمت دسته سوم آنها در نظر گرفته شده است.

۰-۳ مقایسه با سایر استانداردهای مرتبط با روند ممیزی سوابق الکترونیکی سلامت

این استاندارد ملی مطابق با الزامات استاندارد ISO 27799:2008 است تا آنجاکه آنها در ارتباط به ممیزی و روند ممیزی است.

برخی خوانندگان ممکن است با سامانه نیروی کار مهندسی اینترنت (IETF)[3] درخواست نظر (RFC)[4] ۳۸۸۱ آشنایی داشته باشند. (خوانندگانی که با IETF RFC 3881 آشنایی ندارند نیازی به مراجعه به آن سند

1 - Field
2 -A Point in Time
3 - Internet Engineering Task Force
4 -Request For Comment

ندارند زیرا آشنایی با سند مذکور به‌منظور درک این استاندارد ملی موردنیاز نیست). اطلاعات RFC 3881 ثبت‌شده در تاریخ ۰۹-۲۰۰۴ که به‌طور فعال در پایگاه داده IETF وجود ندارد اولین تلاش کارآمد در راستای تعیین محتوای سیاههٔ ممیزی برای بهداشت و درمان است. تا حد امکان، این استاندارد ملی بر همین مبنا بوده و با اقدامات آغاز شده در RFC 3881 در زمینه دسترسی به EHR هماهنگ است.

۰-۴ نکته‌ای در مورد واژگان

چند کلمهٔ مرتبط در بند ۳ مطرح شده‌اند. *سیاههٔ ممیزی* به‌صورت ترتیب زمانی *سوابق ممیزی* تعریف می‌شود. هر سابقه ممیزی شامل شواهدی می‌شود که یا به‌صورت مستقیم وابسته به یک عملکرد یا فرآیند سامانه هستند و یا از آن ناشی می‌شوند. همان‌طور که سامانه EHR می‌تواند مجموعه‌ای پیچیده از سامانه‌ها و پایگاه داده‌ها باشد این امکان وجود دارد که بیش از یک سیاههٔ ممیزی شامل اطلاعات مربوط به وقایع سامانه باشد که باعث تغییر در EHR یک فرد تحت مراقبت شده است. هرچند واژه‌های *روند ممیزی* و *سیاههٔ ممیزی* معمولاً به‌جای هم به‌کاربرده می‌شود اما در این استاندارد ملی واژه *روند ممیزی* به‌عنوان مجموعه‌ای از کلیه سوابق ممیزی مربوط به یک یا چند سیاههٔ ممیزی که مرتبط با یک فرد تحت مراقبت ویژه و یا سوابق الکترونیک سلامت خاص و یا کاربر خاص باشد را شامل می‌شود. یک سامانه ممیزی تمامی کارکردهای پردازش اطلاعات موردنیاز برای نگهداری یک یا چند سیاههٔ ممیزی را شامل می‌شود.

داده‌ورزی سلامت – روندهای ممیزی برای سوابق الکترونیکی سلامت

۱ هدف و دامنهٔ کاربرد

هدف از تدوین این استاندارد، تعیین چارچوب مشترک برای روندهای ممیزی سوابق الکترونیکی سلامت ازنظر رویدادهای سبب‌ساز ممیزی و داده ممیزی برای نگهداری مجموعه کاملی از اطلاعات سلامت شخصی قابل ممیزی در سامانه‌های اطلاعاتی و دامنه‌های مربوط است.

این استاندارد، در سامانه‌هایی کاربرد دارد که قادر به پردازش اطلاعات سلامت شخصی افراد باشد که مطابق با استاندارد ISO 277799 است و سابقه ممیزی امنی را در هر زمان فراهم کرده و در اختیار کاربر قرار می‌دهد. علاوه بر این، این استاندارد از طریق سامانه قادر به ایجاد، به‌روزرسانی و بایگانی اطلاعات سلامت شخصی است.

یادآوری- چنین سوابق ممیزی، حداقل قادر به شناسایی شخص تحت مراقبت و شناسایی عملکرد انجام‌شده توسط کاربر (ایجاد سابقه، دسترسی، به‌روزرسانی و غیره) و ثبت تاریخ و زمانی که عمل انجام‌شده، می‌باشد.

این استاندارد، تنها اقدامات انجام‌شده در راستای EHR را پوشش می‌دهد که از طریق سیاست دسترسی برای حوزه‌ای که در آنجا ثبت الکترونیکی سلامت مستقر است، اداره می‌شود. این استاندارد با هیچ‌یک از اطلاعات سلامت شخصی به‌دست‌آمده از ثبت الکترونیک سلامت سروکار ندارد، به‌غیراز شناساگرها، ثبت ممیزی تنها حاوی پیوندهایی به بخش EHR است که توسط سیاست دسترسی حاکم تعریف شده است.

این استاندارد ذکر خصوصیت و استفاده از سیاهه ممیزی برای مدیریت سامانه و اهداف امنیتی سامانه، نظیر تشخیص مشکلات عملکرد، نقص کاربرد یا پشتیبانی از ساخت داده‌ای که تنها توسط استانداردهای امنیتی کلی رایانه، مانند ISO/IKEC 15408-2 قابل‌بررسی است را پوشش نمی‌دهد [۹].

۲ مراجع الزامی

استفاده از مراجع زیر برای این استاندارد الزامی است. درصورتی‌که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدیدنظرهای بعدی آن موردنظر این استاندارد ملی ایران نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدیدنظر و اصلاحیه‌های بعدی آن‌ها موردنظر است.

۱- ISO 8601:2004، عناصر داده[1] و قالب‌های تبادل[2]، تبادل اطلاعات، ارائه تاریخ و زمان

1 - Data elements
2 - Interchange formats

۲- ISO 27799:2008، داده‌ورزی سلامت، مدیریت امنیت اطلاعات در سلامت با استفاده از ISO/IEG27002

۳ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف زیر به کار می‌رود:

۱-۳

واپایش[1] دسترسی

ابزاری است که دسترسی به اموال و اسناد مجاز را تضمین کرده و بر مبنای الزامات امنیتی و کسب‌وکار محدود می‌کند.

[ISO/IEG 27000:2012, DEFINITION 2.1]

۲-۳

سیاست دسترسی

تعریف تعهدات دسترسی مجاز به منبع است.

۳-۳

جوابگویی[2]

اصلی که نشان می‌دهد، افراد، سازمان‌ها و جامعه مسئول اعمال خود بوده و ممکن است نیاز باشد آن را برای سایرین شرح دهد.

[ISO 15489-1:2001, DEFINITION 3.2]

۴-۳

ممیزی

بررسی سامانه‌ای و مستقل دسترسی‌ها، افزونه‌ها و جایگزین‌های مربوط به سوابق الکترونیکی سلامت و تعیین این مسئله که آیا فعالیت‌های انجام‌شده، داده‌هایی که گردآوری شده، استفاده شده، حفظ شده یا افشا شده مطابق با استاندارد سازمانی و رویه‌های کاری، سیاست‌ها، اصول بالینی بهینه و الزامات مقرراتی قابل‌اجرا است یا خیر.

---

1 - Control
2 - Accountability

۵-۳

بایگانی ممیزی

جمع‌آوری مجموعه‌ای از یک یا چند نمونه از سیاهه‌های ممیزی است.

۶-۳

داده ممیزی

داده‌های به‌دست‌آمده از یک یا چند سابقه ممیزی است

۷-۳

سیاهه ممیزی

توالی همزمان از سوابق ممیزی که هر یک از آنها حاوی داده مربوط به یک رویداد خاص است.

۸-۳

سابقه ممیزی

ثبت یک رویداد ویژه منفرد در دوره طول عمر سابقه الکترونیکی سلامت است.

۹-۳

سامانه ممیزی

سامانه پردازش اطلاعاتی که یک یا چند سیاهه ممیزی را حفظ می‌کند.

۱۰-۳

روند ممیزی

مجموعه اسناد ممیزی از یک یا چند سیاهه ممیزی، مربوط به یک شخص خاص تحت مراقبت یا یک سابقه الکترونیکی سلامت ویژه است.

۱۱-۳

تشخیص هویت[1]

تمهیدات تضمینی است که نشان می‌دهد مشخصه ادعاشده یک موجودیت صحیح است.

---

1 - Authentication

[ISO/IEC27000:2012, DEFINITION2.8]

۱۲-۳

مجوز[1]

اعطای امتیازاتی که کل اعطای امتیازات دسترسی به داده و کارکردها را شامل می‌شود.

یادآوری - با توجه به استاندارد ISO 7498-2، اعطای حقوقی که دسترسی را بر مبنای حقوق دسترسی شامل می‌شود.

۱۳-۳

مرجع صلاحیت‌دار[2]

نهادی که مسئول صدور گواهینامه است.

۱۴-۳

دسترس‌پذیری

خصوصیتی که قابل‌دسترس و استفاده است و از سوی نهاد مجاز، تقاضا می‌شود.

[ISO/IEC 27000:2012, DEFINITION 2.10]

۱۵-۳

محرمانگی

ویژگی‌ای که نشان می‌دهد اطلاعات برای افراد، موجودیت‌ها یا فرآیندهای غیرمجاز قابل دسترس یا ارائه نیست.

[ISO/IEG 27000:2012, DEFINITION 2.13]

۱۶-۳

وقت جهانی تنظیم‌شده

UTC[3]

مقیاس زمانی که بر مبنای پخش رادیویی هماهنگ بسامدهای استاندارد و نشانک‌های زمانی تشکیل شده، دقیقاً با نرخ زمانی اتمی بین‌المللی در ارتباط است، اما در عدد صحیح ثانیه متمایز از آن است.

[IEC 60050-713:1998]

---

1 - Authorization
2 - Authority
3 - Coordinated Universal Time

۱۷-۳

یکپارچگی داده

ویژگی که نشان می‌دهد داده‌ها به روش غیرمجاز تغییر نکرده یا از بین نرفته است.

[ISO 7498-2:1989, DEFINITION 3.3.21]

۱۸-۳

سابقه الکترونیکی سلامت

EHR

مجموعه‌ای جامع و ساخت‌یافته از داده‌های مالی، اجتماعی، محیطی، آماری و بالینی به شکل الکترونیک که مراقبت از بهداشت و سلامت شخص را به‌صورت فردی مستند می‌کند.

[ASTM E1769: 1995]

۱۹-۳

بخش[1] HER

بخشی از EHR که به‌منزلهٔ یک منبع مجزا از سیاست دسترسی است.

۲۰-۳

شناسایی

عملکرد آزمایش‌ها به‌منظور توانمندسازی سامانه پردازش داده در خصوص تشخیص موجودیت‌ها است.

[ISO/IEC 2382-8:1998.DEFINITION 08.04.12] (مانند شناسایی هویت و تشخیص اعتبار هویت)

۲۱-۳

شناسه

بخشی از اطلاعات مورداستفاده برای ادعای هویت قبل از تائید از سوی تأییدکننده مربوط است.

۲۲-۳

امنیت اطلاعات

حفظ محرمانگی، یکپارچگی و دسترس‌پذیری اطلاعات است.

---

1 - Segment

[ISO/IIEC 27000:2012, DEFINITION 2.30]

۲۳-۳

یکپارچگی

خصوصیت حفاظت دقیق و کامل از دارایی‌ها است.

[ISO/IEC 27000:2012, DEFINITION 2.36]

۲۴-۳

شناسه اشیاء (اسناد)

OID [1]

شناسه منحصربه‌فرد جهانی برای یک مجموعه اطلاعات خاص است.

یادآوری- شناسه‌های اشیاء (اسناد) به‌کاررفته در این استاندارد بر سامانه‌های کدگذاری دلالت دارد. این سامانه‌های کدگذار ممکن است در هر اجرا طبق الزامات بین‌المللی استاندارد یا محلی تعریف شوند. شناسه اشیاء (اسناد) با استفاده از نماد انتزاعی نحو[2] (ASN.1) تعریف‌شده در ISO/IEC 8824-1 و ISO/IEC8824-2 مشخص می‌شود.

۲۵-۳

سیاست

مجموعه‌ای از تعهدات قانونی، سیاسی، سازمانی، کاربردی و فنی نسبت به ارتباطات، مشارکت و همکاری است.

[ISO/TS 22600]

۲۶-۳

امتیاز[3]

حق داده شده به یک موجودیت از سوی مقام صلاحیت‌دار است.

1 - Object identifier
2 - Abstract Syntax Notation
3 - Privilege

۲۷-۳

مدیریت سوابق

زمینه مدیریتی که مسئول واپایش سامانه‌ای و کارآمد ایجاد، دریافت، حفظ، استفاده و تنظیم اسناد و سوابق است، ازجمله فرآیند ضبط و حفظ مدارک و داده مربوط به فعالیت‌های کسب‌وکار و تراکنش‌های ذکرشده در قالب سوابق و مدارک است

[ISO 15489-1, DEFINITTION, 3.16]

۲۸-۳

نقش

مجموعه‌ای از شایستگی‌ها و/ یا کارائی‌های مرتبط به یک وظیفه است.

۲۹-۳

حساسیت

سنجش پتانسیل یا پتانسیل درک شده برای آسیب‌رسانی به مفاد داده یا سوءاستفاده از داده‌ها و استفاده نادرست از آنها است.

۳۰-۳

سیاست امنیت

طرح یا دوره عمل تائید شده در خصوص برقراری امنیت رایانه است.

[ISO/IEC 2382-8:1998.DEFINITION, 08.01.06]

۳۱-۳

شخص تحت مراقبت[1]

شخصی که طبق برنامه زمان‌بندی، نیاز به دریافت خدمات بهداشتی داشته یا الزاماً باید آنها را دریافت کند.

[ISO 18308:2011,DEFINITION 3.47]

1 - Subject of care

۳۲-۳

کاربر

شخص، افزاره[1] یا برنامه‌ای که از سامانه EHR برای پردازش داده یا تبادل اطلاعات بهداشتی و سلامتی استفاده می‌کند.

۴ نمادها و کوته‌نوشت‌ها

EHR سابقه الکترونیکی سلامت

HL7 هفتمین سطح استاندارد بین‌المللی سلامت

OID شناسه اشیاء (اسناد)

UTC زمان جهانی هماهنگ‌شده

۵ الزامات و کاربردهای داده ممیزی

۵-۱ الزامات رسمی و اخلاقی

۵-۱-۱ کلیات

ارائه‌دهندگان مراقبت‌های بهداشتی، مسئولیت‌های حرفه‌ای و اخلاقی دارند که باید آنها را به اجرا رسانند. آنها از حریم شخصی افراد تحت مراقبت محافظت کرده و یافته‌ها و فعالیت‌های مراقبتی خود را مستندسازی می‌کنند. محدودیت دسترسی به سوابق سلامت و حصول اطمینان از استفاده مناسب از آنها، هر دو از الزامات اساسی در مراقبت‌های بهداشتی هستند و در بسیاری از حوزه‌های قضائی این نیاز در متن قانون درج شده است.

روندهای ممیزی امن از دسترسی به سوابق الکترونیکی سلامت ممکن است منطبق با اصول اخلاقی حرفه‌ای، سیاست‌های سازمانی، قوانین و مقررات باشد، اما آنها به تنهایی برای ارزیابی کامل سوابق الکترونیکی سلامت کافی نیست.

۵-۱-۲ سیاست دسترسی

سازمانی که مسئول حفظ و نگهداری یک سیاهه ممیزی است، باید سیاست دسترسی حاکم بر همهٔ دسترسی‌های ثبت شده را شناسایی کند.

---

1 - Device

سیاست دسترسی باید مطابق با زیربندِ ۷-۸-۱-۱ استانداردِ ISO 27799:2008 با عنوان سیاست واپایش دسترسی باشد.

یادآوری ۱- فرض شده است این سیاست دسترسی، یک ساختار بخش EHR را تعریف می‌کند.

یادآوری ۲- در سابقه ممیزی، سیاست دسترسی از طریق منبع سیاهه ممیزی مشخص می‌شود.

راهنمای مربوط به تعیین و پیاده‌سازی سیاست‌های دسترسی می‌تواند در استاندارد ISO/TS 22600 یافت شود [۶]. فیلد «Participant object Permission PolicySet» در 7.66 تعریف شده و بر سیاست‌های واقعی اعمال شده در سوابق ممیزی دلالت دارد.

۵-۱-۳ تشخیص دقیق کاربران سامانه اطلاعات

روند ممیزی باید اطلاعات کافی برای شناسایی بدون ابهام، همهٔ اطلاعات سلامت را به کاربران مجاز سامانه ارائه کند. کاربران سامانه اطلاعاتی می‌توانند اشخاص یا سایر موجودیت‌ها باشند.

روندهای ممیزی باید اطلاعات کافی برای تعیین اینکه کدام کاربرانِ مجاز و سامانه‌هایِ خارجی دسترسی داشته‌اند و یا اطلاعات سابقه سلامت را از سامانه ارسال کرده‌اند را ارائه کنند.

۵-۱-۴ نقش کاربران

روند ممیزی، باید نقش کاربر را در حین انجام عمل ثبت شده روی اطلاعات شخصی سلامت، نشان دهد.

سامانه‌های اطلاعاتی که اطلاعات سلامت شخصی را پردازش می‌کنند، بهتر است از واپایش دسترسی مبتنی بر نقش، پشتیبانی کرده و امکان انجام یک یا چند نقش را به هر کاربر و هر نقش را به یک یا چند کارکرد سامانه نگاشت کند (همان‌طور که در بخش مدیریت امتیاز انحصاری در استاندارد ISO 27799:2008، ۷-۸-۲-۲ شرح داده شده است).

نقش‌های ساختاری و کاربردی در استاندارد ISO/TS21298 مستند شده است [۴]. راهنمای اضافی مربوط به مدیریت امتیاز انحصاری سلامت و بهداشت، توسط استاندارد ISO/TS22600 ارائه می‌شود (تمام بندها) [۶].

۵-۱-۵ سوابق ممیزی امن

سوابق ممیزی امن باید هر زمان که اطلاعات شخصی سلامت دیده شده، ایجاد شده، به‌روز شده یا بایگانی شود، منطبق با ISO27799:2008، ۷-۷-۱۰-۲، ایجاد شوند. سوابق ممیزی اساساً باید توسط مدیریت امن سوابق، حفظ و نگهداری شوند.

۵-۲ استفاده از داده ممیزی

۵-۲-۱ حاکمیت و نظارت

روند ممیزی باید داده‌هایی را فراهم کند تا مراجع مسئول را قادر سازد انطباق آن با سیاست سازمانی را بررسی کرده و تأثیرات آن را ارزیابی کنند.

این امر بر مسائل ذیل اشاره دارد:

- تشخیص دسترسی غیرمجاز به سوابق بهداشت و سلامت،
- ارزشیابی دسترسی اضطراری،
- تشخیص و کشف سوءاستفاده از حقوق و امتیاز انحصاری،

و از موارد ذیل پشتیبانی می‌کند:

- مستندسازی دسترسی از طریق دامنه‌ها، و
- ارزشیابی سیاست‌های دسترسی

یادآوری- ارزیابی کلی انطباق با سیاست سازمان می‌تواند به داده‌های اضافی نیاز داشته باشد که آنها در این سابقه ممیزی قرار نگرفته و آن را شامل نمی‌شوند، به‌طور مثال اطلاعات کاربر، جدول مجوزها یا سوابق ورود فیزیکی به اتاق‌های امنیتی. برای کسب اطلاعات بیشتر از خدمات سیاهه ممیزی به پیوست ب مراجعه کنید.

روند ممیزی باید داده کافی برای تعیین همهٔ دسترسی‌ها در بازه زمانی تعریف شده به سوابق شخص تحت مراقبت به‌وسیلهٔ یک کاربر خاص را فراهم کند.

روند ممیزی باید داده کافی برای تعیین همهٔ دسترسی‌ها در بازه زمانی تعریف شده به سوابق اشخاص تحت مراقبت که در معرض خطر بالای نقض حریم خصوصی علامت‌گذاری شده را فراهم کند.

۵-۲-۲ اشخاص تحت مراقبت از حقوقشان استفاده می‌کنند

روند ممیزی باید داده کافی برای شخص تحت مراقبت را فراهم کند و امکان کارهای ذیل را میسر کند:

- ارزیابی که نشان می‌دهد کدام کاربر (کاربران) مجاز، به سابقه بهداشت و سلامت خود و در چه زمانی دسترسی داشته است،
- ارزیابی جوابگویی برای محتوای سابقه،
- تعیین انطباق با بخشنامه موافقت شخص تحت مراقبت برای دسترسی یا افشای داده شخص تحت مراقبت، و
- تعیین دسترسی اضطراری (در صورت وجود) واگذار شده به کاربر برای سابقه شخص تحت مراقبت، ازجمله شناسایی کاربر، زمان دسترسی و محلی که از آن دسترسی صورت گرفته است.

۵-۲-۳ اصول اخلاقی ارائه‌دهنده مراقبت‌های بهداشتی و سلامت و اقدامات حقوقی و قانونی صورت‌گرفته از سوی آنها

روند ممیزی باید داده و شواهد مستندی از اینکه چه اطلاعاتی دیده شده است و چه اقداماتی صورت گرفته است را ارائه دهد (ایجاد، مشاهده، مطالعه، تصحیح، به‌روزرسانی، استخراج، برونداد، بایگانی اطلاعات و غیره) که تمامی این موارد با اطلاعات چه زمانی و توسط چه کسی در ارتباط است.

حفظ و نگهداری سوابق ممیزی بهتر است همسو با شرایط قانونی جوابگویی در حوزه قضائی باشد.

برای کسب اطلاعات بیشتر به بخش مدیریت سوابق HL7 EHR و پشتیبانی شواهد مراجعه نمایید (RM-ES).

۶ رویدادهای سبب‌ساز[1]

۶-۱ کلیات

رویدادهای ممیزی (رویدادهای سبب‌ساز) که باعث ایجاد سوابق ممیزی در سامانه ممیزی می‌شوند، طبق مقیاس هر سامانه اطلاعات بهداشت و سلامت، هدف و محتویات اطلاعات خصوصی و سیاست‌های امنیتی تعریف می‌شوند. هدف و دامنه کاربرد این استاندارد ملی دسترسی به اطلاعات شخصی بهداشت و سلامت افراد محدود می‌شود. تنها رویدادهای سبب‌ساز مربوط به دسترسی در اینجا مشخص شده است.

دو رویداد ذیل به‌منظور تهیه سوابق ممیزی مانند چه زمانی، مال چه کسی، چه کسی و انطباق آنها با الزامات منتج شده از بند ۵ (الزامات و استفاده از اطلاعات ممیزی) اجباری است.

الف- رویدادهای دسترسی به اطلاعات شخصی سلامت

ب- رویدادهای پرس‌وجوی اطلاعات شخصی سلامت

مثال‌هایی مربوط به رویدادهای خارج از این زمینه در ذیل مطرح شده است:

- رویدادهای شروع و توقف برنامه کاربردی؛
- رویدادهای احراز هویت شامل احراز هویت کاربران؛
- رویدادهای ورودی و خروجی از/به محیط خارجی؛
- رویدادهای دسترسی به اطلاعاتی به‌جز اطلاعات شخصی بهداشت و سلامت؛
- رویدادهای هشدار امنیتی مربوط به برنامه‌های کاربردی؛
- رویدادهای دسترسی به سیاهه ممیزی نگهداری شده در برنامه‌های کاربردی؛
- رویدادهای تولید شده توسط سیستم‌عامل، میان‌افزار و غیره؛

---

1 - Trigger events

- رویدادهای دسترسی ایجاد شده به‌وسیلهٔ خدمات عمومیِ سامانه‌ای؛
- رویدادهای قطع یا وصل ارتباط فیزیکی تجهیزات متصل شده به شبکه؛
- رویدادهای شروع یا توقف سامانه‌های حفاظت، به‌طور مثال سامانه‌های حفاظت ضد ویروس؛
- رویدادهای به‌روزرسانی نرم‌افزار شامل برنامه‌های اصلاح نرم‌افزار یا برنامه‌های وصله.

۶-۲ جزئیات مربوط به انواع رویدادها و محتویات آنها

۶-۲-۱ رویدادهای دسترسی به اطلاعات شخصی بهداشت و سلامت

در این استاندارد ملی، دسترسی به اطلاعات شخصی بهداشت و سلامت یک رویداد ممیزی قلمداد می‌شود. این دسترسی[1] به معنی ایجاد، مطالعه، به‌روزرسانی و حذف داده است. محتویات مربوط به سیاهه ممیزی، اطلاعات مربوط به اینکه دسترسی به داده‌ای که محافظت شده، در چه زمان، توسط چه کسی و «دسترسی به چه کسی» صورت گرفته را ارائه می‌کند. جدول ۱ را مشاهده نمایید.

جدول ۱- رویدادهای دسترسی

رویداد	محتویات
رویدادهای دسترسی به اطلاعات شخصی بهداشت و سلامت	چه زمانی، چه کسی، دسترسی به چه کسی

۶-۲-۲ رویدادهای پرس و جوی اطلاعات شخصی بهداشت و سلامت

پرس‌وجوی یک پایگاه داده EHR به‌منظور کسب اطلاعات شخصی بهداشت و سلامت، به‌عنوان یک رویداد قابل ممیزی در نظر گرفته می‌شود. این رویداد پرس‌وجو خودش یک عمل پرس‌وجو است که به اطلاعات شخصی بهداشت و سلامت اشاره کرده و نتایج حاصل از پرس‌وجو به‌عنوان یک عمل دسترسی نیز در نظر گرفته می‌شود. محتویات یک سابقه ممیزی، اطلاعات مربوط به اینکه پرس‌وجو در چه زمانی، توسط چه کسی و «در چه شرایطی برای پرس‌وجو» صورت گرفته است، فراهم می‌کند. جدول ۲ را ببینید.

جدول ۲- رویدادهای پرس‌وجو

رویداد	محتویات
رویدادهای پرس‌وجو برای اطلاعات شخصی بهداشت و سلامت	چه زمانی، چه کسی، در چه شرایطی برای پرس‌وجو

1 - Access

۷ جزئیات مربوط به سابقه ممیزی

۷-۱ قالب کلی سابقه

جدول ۳، قالب کلی سوابق ممیزی را شرح می‌دهد. با توجه به محتویات سابقه از هر رویداد، بند ۸ را ببینید. قالب سابقه پس از RFC3881 [۱۳] و DICOM [۱۱] با اضافه کردن فیلدهای اختیـاری PurposeOfUse و ParticipantObjectPolicySet تعریف شده است.

جدول ۳- قالب کلی سوابق ممیزی

نوع	نام فیلد	گزینه	توضیح	اطلاعات اضافی
رویداد مربوط به (۱)	EventID	M	ID به‌کاررفته در رویداد ممیزی شده	به ۷-۲ مراجعه کنید
	EventActionCode	M	نوع عمل اجرا شده در طول رویداد ممیزی شده	
	EventDateTime	M	تاریخ/زمان وقوع رویداد	
	EventOutcomeIndicator	U	موفقیت یا شکست رویداد	
	EventTypeCode	U	طبقه رویداد	
کاربر مربوط به (۲..۱)	UserID	M	ID شخص یا فرآیند	به ۷-۳ مراجعه کنید.
	AlternateUserID	U	ID جایگزین برای کاربر یا فرآیند	
	UserName	U	نام کاربر یا فرآیند	
	UserIsRequestor	U	شاخصی که نشان می‌دهد کاربر درخواست‌کننده است یا خیر.	
	RoleIDCode	U	مشخصات نقش کاربر در هنگام انجام یک رویداد	
	PurposeOfUse	U	کد مربوط به هدف از استفاده از داده در دسترس قرار داده شده	
	NetworkAccessPointTypeCode	U	نوع نقطه دسترسی به شبکه	به ۷-۴ مراجعه کنید
	NetworkAccessPointID	U	ID نقطه دسترسی به شبکه	
سامانه ممیزی مربوط به (۱)	AuditEnterpriseSiteID	U	ID محل شرکت ممیزی	به ۷-۵ مراجعه کنید
	AuditSourceID	M	ID منحصربه‌فرد منبع ممیزی	
	AuditSourceTypeCode	U	نوع کد منبع ممیزی	
مفاد مربوط به شخص شرکت‌کننده (0…N)	ParticipantObjectTypeCode	M	کد مربوط به نوع شیء شرکت‌کننده	به ۷-۶ مراجعه
	ParticipantObjectTypeCodeRole	M	کد نوع شیء نقش	
	ParticipantObjectDataLifeCycle	U	شناسه به‌کاررفته در مرحله طول عمر داده	

نوع	نام فیلد	گزینه	توضیح	اطلاعات اضافی
			برای شیء شرکت‌کننده	کنید.
	ParticipantObjectIDTypeCode	M	کد نوع ID شیء شرکت‌کننده	
	ParticipantObjectPolicySet	U	مجموعه سیاست اجازه دسترسی برای ParticipantObjectID	
	ParticipantObjectSensitivity	U	حساسیت‌پذیری تعریف شده از طریق سیاست اعمال شده برای ParticipantObjectID	
	ParticipantObjectID	M	شناسایی و تشخیص مثال خاصی از شیء شرکت‌کننده	
	ParticipantObjectName	U	نام شیء شرکت‌کننده، به‌طور مثال نام شخص	
	ParticipantObjectQuery	M/U	محتویات پرس‌وجو برای شیء شرکت‌کننده	
	ParticipantObjectDetail	U	جزئیات شیء شرکت‌کننده	
تعدد		**گزینهٔ انتخابی**		
۱		M	اجباری	
(0..1)	۰ یا ۱ موجود است.	MC	اجباری مشروط	
(1..2)	۱ یا ۲ موجود است.	U	اختیاری	
(0…N)	۰ تا N موجود است.	M/U	اختیاری یا اجباری بسته به رویدادها	

۷-۲ شناسایی رویدادهای سبب‌ساز

۷-۲-۱ شناسه رویداد[1]

توضیح: شناسه منحصربه‌فرد برای یک رویداد ممیزی خاص، مانند: یک عنوان از قلم انتخابی[2]، برنامه، قانون، سیاست، کد وظیفه[3]، نام برنامه کاربردی یا URL است. این شناسه کارکرد انجام شده را شناسایی می‌کند.

گزینهٔ انتخابی[4]: اجباری[5]

1 - Event ID
2 - Menu item
3 - Function
4 - Optionality
5 - mandatory

قالب/مقادیر: مقدار کد شده، به هر دو صورت، هم به‌وسیلهٔ مجریان سامانه و هم به‌عنوان یک مرجع استاندارد واژگان تعریف می‌شود. خصیصه کد دست‌کم در شناسه منبع ممیزی[1] باید بدون ابهام و منحصربه‌فرد باشد. (۷-۵ را مشاهده کنید). مثال‌های مربوط به Event ID عبارت است از: نام برنامه، نام روش یا نام تابع.

یادآوری - کدگذاری پس از IHE ITI TF-1 و TF-2[۱۲]، ISO 12052، [۱]، DICOMپیوست 95[۱۱] الگوبرداری می‌شود.

در پیاده‌سازی، برای مقادیر کدشده یا ارجاع به استانداردها، طرح‌وارهٔ[2] XML مطرح شده در RFC3881 ویژگی‌های اختیاری مانند آنچه در جدول ۴ نشان داده شده را تعریف می‌کند.

جدول ۴: ویژگی‌های منبع Event ID

ویژگی[3]	مقدار
CodeSystem	مرجع OID
CodeSystemName	نام سامانه کدگذاری، به شدت توصیه می‌شود که برای مجموعه کد به‌صورت محلی تعریف شده و ارزش‌گذاری شود
CodeValue	کد ویژه به‌کاررفته در سامانه کدگذاری
DisplayName	مقدار ارزش به‌کاررفته در گزارش‌ها و نمایش‌ها
OriginalText	مقدار ورودی که به کد تبدیل شده است

به‌منظور حمایت و پشتیبانی از نیاز به شناسایی رویداد بدون ابهام، چند مقدار ممکن است مشخص نشود.

مبنای منطقی[4]:

شناسه، تابع ممیزی شده را شناسایی می‌کند. به‌علاوه، به‌منظور اجرای کد عمل رویداد سوابق ممیزی، کارکرد برنامه کاربردی انجام‌شده را نیز مشخص می‌کند.

حداقل، یکی از کد سامانه ((CodeSystem (OID)) یا نام کد سامانه (CodeSystemName) اجباری است.

۷-۲-۲ کد فعالیت رویداد[5]

توضیح: شناسه برای نوع فعالیت انجام‌شده در رویداد ممیزی

گزینهٔ انتخابی: اجباری

---

1 - Audit Source ID
2 -Schema
3 - Attribute
4 - Rationale
5 - Event action code

قالب/مقادیر: برشماری که در جدول ۵ نشان داده شده است.

جدول ۵- کدهای عمل رویداد[1]

مقدار	مفهوم	مثال‌ها
C	ایجاد	ایجاد شیء جدید پایگاه داده، به‌طور مثال قرار دادن یک دستور
R	مطالعه/دیدن/ چاپ /پرس‌وجو	نمایش یا چاپ داده، به‌طور مثال یک تشخیص
U	به‌روزرسانی	به‌روزرسانی داده، به‌طور مثال اصلاح اطلاعات سلامت و بهداشت شخصی
D	حذف	غیرقابل‌دسترس کردن قلم‌ها[2]
E	اجرا	اجرای یک سامانه یا تابع برنامه کاربردی، به‌طور مثال جستجو، استخراج، یا استفاده از روش یک شیء[3]

مبنای منطقی: به‌طورکلی نشان می‌دهد که چه نوع عملی روی شیء شرکت‌کننده انجام شده است.

یادآوری ۱- اقداماتی که در بالا برشمرده نشده است در بخش اجرای یک تابع خاص یا روش رابط شیء یا مورد عمل قرار دادن دو یا چند رویداد مجزا، در نظر گرفته شده‌اند. یک فعالیت کاربردی مانند صدور مجوز یا امضای دیجیتال، یک تابع اجرایی است و Event ID، تابع را شناسایی خواهد نمود.

یادآوری ۲- برای برخی برنامه‌های کاربردی، به‌طور مثال تصویربرداری رادیولوژی، یک عمل پرس‌وجو می‌تواند تنها وجود داده را تعیین کند، اما دسترسی به خود داده مقدور نیست. ممیزی معمولاً نیازی به این تمایز ندارد.

یادآوری ۳- اقدامات ترکیبی مانند «جابجایی»، «بایگانی» یا «رونوشت۴» می‌تواند از طریق ایجاد داده ممیزی برای هر یک از عملیات خواندن، ایجاد، حذف یا به‌عنوان اجرای یک تابع یا روش ممیزی شود.

۷-۲-۳ تاریخ و زمان رویداد[5]

توضیح: تعیین تاریخ/زمانی که مشخص بوده و منطبق با بازه زمانی منطقه است.

گزینهٔ انتخابی: اجباری

1 - Event action codes
2 - Items
3 - object’s method
4 - Copy
5 - Event date and time

قالب/مقادیر: ارائه زمان/ تاریخ دقیق برحسب زمان هماهنگ‌شده جهانی صورت می‌گیرد (UTC). این زمان در قالب UTC است و به شکل استاندارد ISO 8601:2004 نشان داده می‌شود. بازه تغییرات آنها نباید بیشتر از ۲۵۰ میلی‌ثانیه در قالب UTC باشد.

مبنای منطقی: این روش، رویداد را به یک تاریخ و زمان خاص مرتبط می‌سازد. ممیزی‌های امنیتی به‌طور نمونه به یک بازه زمانی پایدار نیاز دارد، مخصوصاً در خصوص حذف مسائل بازه زمانی ناشی از ویژگی جغرافیایی.

یادآوری- در یک سامانه توزیع شده، برخی بازه‌های زمانی مثل کارساز[1] (NTP(RFC1305، روش اجرای مطلوب محسوب می‌شوند.

۷-۲-۴ شاخص نتیجه رویداد[2]

توضیح: این شاخص مشخص می‌کند که رویداد به‌طور موفقیت‌آمیز به وقوع پیوسته است یا خیر.

گزینهٔ انتخابی: اختیاری

قالب/مقادیر: مقادیر کدگذاری شده: کد صفر (۰) نشان‌دهندهٔ موفقیت است. مقادیر مربوط به شکست رویداد در هدف و دامنه کاربرد این استاندارد بدون معنا می‌باشند.

مبنای منطقی: این فیلد به‌منظور حفظ سازگاری با روند ممیزی تعریف‌شده در IETF RFC 3881، مشخص شده است.

۷-۲-۵ کد نوع رویداد[3]

توضیح: شناسه برای طبقه رویداد

گزینهٔ انتخابی: اختیاری

قالب/مقادیر: برشماری مقدار کدگذاری شده از نوع شمارشی که به‌وسیلهٔ مجریان سامانه یا مرجع اصطلاحات و واژگان استاندارد تعریف شده است. برای پیاده‌سازی کدهای تعریف شده[4]، یا منابع مربوط به استانداردها، طرح‌وارهٔ[5] XML در RFC3881، ویژگی‌های اختیاری را مانند آنچه در جدول ۶ نشان داده شده، تعریف می‌کند.

1 - Server
2 - Event outcome indicator
3 - Event type code
4 - Implementation-defined codes
5 - Schema

جدول ۶- ویژگی‌های مرجع کد نوع رویداد[1]

صفت	مقدار
CodeSystem	مرجع OID
CodeSystemName	نام سامانه کدگذاری، به شدت توصیه می‌شود که برای مجموعه کد به‌صورت محلی تعریف شده و ارزش‌گذاری شود
DisplayName	مقدار و مقدار به‌کاررفته در گزارش‌ها و نمایش‌ها
OriginalText	مقدار ورودی به کد ترجمه شده است

ازآنجایی‌که رویدادها ممکن است به بیش از یک روش طبقه‌بندی شوند، ممکن است مقادیر چندگانه مشخص گردد.

مبنای منطقی: این فیلد امکان پرس‌وجو از سوابق ممیزی از طریق رده‌بندی‌های اجرامحور رویداد را فراهم می‌کند.

۷-۳ احراز هویت کاربر[2]

۷-۳-۱ شناسه کاربر[3]

توضیح: شناسه منحصربه‌فرد برای کاربری که به‌طور فعال در رویداد شرکت کرده است.

گزینهٔ انتخابی: اجباری

قالب /مقادیر: رشته متن شناسه کاربر از سامانه احراز هویت به دست می‌آید. این رشته متن، مقدار منحصربه‌فردی دارد که منطبق با شناسه منبع ممیزی است (بند ۷-۴ را مشاهده کنید).

مبنای منطقی: این فیلد، رویداد ممیزی را به یک کاربر خاص مرتبط می‌سازد. در این زمینه، کاربر ممکن است یک شخص، گروه، تیم، کارساز، فرآیند یا موضوع کار[4] باشد.

یادآوری ۱- برای ممیزی میان سامانه‌ای، مخصوصاً در طول حفظ و نگهداری درازمدت سامانه، این شناسه کاربر به این معنا است که رویداد ممیزی به‌طور دائم از طریق یک کلید منحصربه‌فرد به یک کاربر خاص ربط داده می‌شود. درنتیجه، در کل طول عمر بایگانی روند ممیزی منحصربه‌فرد بودن آن معتبر است.

یادآوری ۲- برای احراز هویت مبتنی بر گره شبکه؛ زمانی که تنها فرآیند یا سخت‌افزار سامانه باید مورد ارزیابی قرار گیرد، اما هیچ کاربر انسانی شناسایی نمی‌شود، شناسه کاربر، می‌تواند نام گره باشد.

1 - Event type code reference attributes
2 - User identification
3 - User ID
4 - Task thread

یادآوری ۳- اگر روند ممیزی برای ممیزی بالینی یا ارائهٔ شواهد، یا آنجا که موردنیاز است مانند موارد سوءاستفاده، به کار رود، روند ممیزی ممکن است نیاز داشته باشد که اطلاعات کافی ثبت نماید برای اینکه ارتباط یک شناسه منحصربه‌فرد را با یک کاربر واقعی به‌روشنی مشخص کند.

۷-۳-۲ شناسه کاربر جایگزین[1]

توضیح: شناسه منحصربه‌فرد جایگزین شده به‌جای کاربر

گزینهٔ انتخابی: اختیاری

قالب/مقادیر: متن شناسه کاربر از سامانه احراز هویت استنتاج شده است. این شناسه برابر با ۱ است و در صورت در دسترس قرار گرفتن به‌طور متداول در سامانه مشخص می‌شود.

مبنای منطقی: در برخی موقعیت‌ها، کاربر ممکن است از طریق یک هویت، تائید اعتبار شود، اما دسترسی به یک سامانه کاربردی ویژه، ممکن است منوط به هویت مشابه باشد. شناسه جایگزین، پس از آنکه به‌عنوان شناسه اصلی بکار رود برای احراز صلاحیت استفاده می‌شود. ID کاربر شناخته شده است و توسط برنامه به کار می‌رود.

۷-۳-۳ نام کاربر[2]

توضیح: نام بامعنی انسان برای کاربر

گزینهٔ انتخابی: اختیاری

قالب/مقادیر: رشته متن

مبنای منطقی: شناسه کاربر[3] یا شناسه کاربر جایگزین[4] ممکن است داخلی باشد یا به‌عبارت‌دیگر، دارای مقادیر مبهمی باشد. این فیلد در تشخیص و شناسایی کاربر واقعی به ممیز کمک می‌کند.

۷-۳-۴ کاربر، درخواست‌کننده است[5]

توضیح: شناسه‌ای که نشان می‌دهد کاربر درخواست‌کننده یا آغازکننده است یا خیر، مخصوصاً در خصوص رویدادهای ممیزی شده.

گزینهٔ انتخابی: اختیاری

قالب/مقادیر: بولین[6]، پیش‌فرض/ مقدار فرض شده «صحیح» است.

---

1 - Alternative user ID
2- User name
3 - User ID
4 - Alternative User ID
5 - User is requestor
6 - Boolean

مبنای منطقی: این مقدار برای ایجاد تمایز بین کاربران درخواست‌کننده و کاربران دریافت‌کننده استفاده می‌شود. به‌طور مثال، یک گزارش می‌تواند توسط یک کاربر بازیابی شود (درخواست‌کننده). یا یک کاربر (درخواست‌کننده) ممکن است خروجی گزارش را تهیه کرده و آن را به کاربر دیگر ارسال کند (کسی که گیرنده گزارش است، اما درخواست‌کننده نیست).

۷-۳-۵ کد شناسه نقش[1]

توضیح: مشخصه نقش (ها) اقدامات کاربر، مخصوصاً وقتی کاربر در حال انجام یک عمل است، با امنیت واپایش دسترسی مبتنی بر نقش در ارتباط است. سامانه‌های واپایش دسترسی مبتنی بر نقش این امکان را به هر کاربر می‌دهند تا یک یا چند نقش را ایفا نماید. هر نقش با یک یا چند کارکرد سامانه در ارتباط است.

گزینهٔ انتخابی: اختیاری، چندمقداره

قالب/مقادیر: مقدار کدگذاری شده، کدی است که بر مبنای کد نقش یا متن به‌دست‌آمده از سامانه ارزش‌گذاری شده است. در این شرایط، بیش از یک مقدار ممکن است مشخص شود، زیرا بیش از یک سامانه واپایش دسترسی مبتنی به نقش وجود دارد، یا اینکه ممکن است طبقه‌بندی مورد استفاده قرار گیرد. یادآوری می‌شود که بند ۷-۸-۲-۲ استاندارد ISO 277799:2008 (مدیریت حقوق انحصاری) و استاندارد ISO/TS 22600 مشخص می‌نمایند که کاربر سامانه اطلاعات بهداشت و سلامت به کل اطلاعات شخصی بهداشت و سلامت اشخاص واقف است و به‌سادگی می‌تواند در یک نقش به خدمات دست یابد (به‌طور مثال، کاربرانی که با بیش از یک نقش، ثبت‌نام کرده‌اند، یک نقش را در طول هر جلسه دسترسی به سامانه اطلاعات بهداشت و سلامت برمی‌گزینند).

توصیه می‌شود از سامانه کدگذاری منطبق با نقش‌های کاربردی تعریف شده در استاندارد ISO/TS21298 [۴] و جدول ۷ استفاده شود.

شناسایی واژگان ذکر شده برای این فهرست از مقادیر کدگذاری شده می‌توانند بر OID ذیل دلالت داشته باشند، آنها از طریق نماد انتزاعی نحو ۱ (ASN.1) تعریف شده در استاندارد ISO/IEC8824-1[۷] و استاندارد ISO/IEC8824-2[۸] تعیین می‌شوند.

شناسایی واژگان: ایزو (۱) استاندارد (۰) نقش‌های ساختاری و کارکردی (۲۱۲۹۸) اصطلاحات و واژگان به‌کاررفته (۴).

1 - Role ID code

جدول ۷- کدهای شناسه نقش کاربردی[1]

شناسه نقش	نام-نقش	توضیح
01	شخص تحت مراقبت	موضوع داده اصلی سوابق الکترونیکی بهداشت و سلامت
02	شخص مراقب	به‌طور مثال، والدین، نگهبان‌ها، مراقب یا سایر نمایندگان حقوقی
03	مراقبت بهداشت و سلامت شخصی	کارشناس حرفه مراقبت از بهداشت و سلامت یا کارشناسان حرفه‌ای با ارتباط نزدیک‌تر با بیمار که اغلب دکتر خانوادگی بیمار است.
04	کارشناس حرفه‌ای مجرب مراقبت از بهداشت و سلامت	منصوب شده از طریق شخص تحت مراقبت یا مسئول یا پرستار منصوب شده از طریق مرکز ارائه خدمات مراقبتی (در صورت معرفی توسط قانون، این کار امکان‌پذیر است، به‌طور مثال شرایط فوریت)
05	کارشناس حرفه‌ای بهداشت و سلامت	طرف درگیر در ارائه مراقبت‌های بهداشتی مستقیم به بیمار
06	کارشناس حرفه‌ای مربوط به بهداشت و سلامت	طرفی که به‌طور غیرمستقیم در امور ذیل شرکت می‌کند، مراقبت از بیمار، آموزش، تحقیق و غیره
07	مدیر اجرایی	سایر طرفین که خدمات ارائه‌شده به بیمار را حمایت می‌نمایند.

این امر فهرست سطح بالایی از نقش‌های کارکردی را فراهم و امکان تبادل سازگار[2] در حیطه اداری و قضائی[3] را ایجاد می‌کند. این روش می‌تواند به‌منظور مدیریت ایجاد، دسترسی، پردازش و ارتباط اطلاعات بهداشت و سلامت به کار رود. بیشتر نقش‌های کارکردی ممکن است منطبق با حوزه قضائی باشند. یا اینکه ممکن است به‌منظور برقراری ارتباط بین زمینه‌ها یا حوزه‌های قضائی تائید شوند.

1 - Functional role ID codes
2 - Interoperable
3 - jurisdictional or domain boundaries

کدها ممکن است تعریف شده در اجرا باشند یا به برشماری واژگان و اصطلاحات استاندارد دلالت داشته باشند. طرح‌واره XML در RFC 3881 به‌منظور اجرای کدها یا مراجع تعریف شده، متغیرهای اختیاری ذکرشده در جدول ۸ را تعریف می‌کند.

جدول ۸- صفت‌های مرجع کد شناسه نقش[1]

صفت	توصیف مقدار
CodeSystem	مرجع OID
CodeSystemName	نام سامانه کدگذاری، به شدت توصیه می‌شود که برای مجموعه کد به‌صورت محلی تعریف شده و ارزش‌گذاری شود.
Display Name	مقدار نشان داده شده در گزارش‌ها و نمایش‌ها
OriginalText	مقدار ورودی به کد ترجمه شده است.

مبنای منطقی: این مقدار، رویداد ممیزی شده را به نقش کاربر مرتبط می‌سازد. این نقش؛ عامل اصلی در سیاست واپایش دسترسی به اطلاعات شخصی بهداشت و سلامت به شمار می‌رود.

راهنمای اضافی می‌تواند در استانداردهای ISO/TS 22600 [۶] و ISO/TS 21298 [۴] یافت شود.

۷-۳-۶ هدف از کاربرد[2]

توضیح: این روش اهدافی را نشان می‌دهد که بر مبنای آن می‌توان فهمید کدام‌یک از اطلاعات شخصی بهداشت و سلامت قابل‌دسترس استفاده خواهند شد.

گزینهٔ انتخابی: اختیاری

قالب /مقادیر: برشماری مقدار کدگذاری شده به‌عنوان مجریان سامانه یا به‌عنوان یک مرجع اصطلاحات و واژگانِ استاندارد تعریف شده است.

توصیه می‌شود سامانه کدگذاری منطبق با طرح‌وارهٔ رده‌بندی اهداف، برای پردازش اطلاعات شخصی بهداشت و سلامت تعریف شده در استاندارد ISO/TS 14265 [۲] و ذکر شده در جدول ۹ مورد استفاده قرار گیرد.

تشخیص واژگان و اصطلاحات ذکر شده در فهرست مقادیر کدگذاری شده می‌تواند بر OID ذیل دلالت نماید. آنها با استفاده از نماد انتزاعی نحو ASN.1 تعریف شده در استاندارد ISO/IEC8824-1 [۷] و ISO/IEC 8824-2 [۸] مشخص می‌شود.

شناسایی واژگان: ایزو (۱) استاندارد (۰) طبقه‌بندی اهداف برای پردازش اطلاعات شخصی بهداشت و سلامت (۱۴۲۶۵) اصطلاحات برای رده‌بندی اهداف برای پردازش اطلاعات شخصی بهداشت و سلامت (۱).

1 - Role ID code reference attributes
2 - Purpose of use

جدول ۹- طبقه‌بندی هدف[1]

کد	اصطلاحات رده‌بندی	توضیح (اطلاعاتی)
۱	ارائه مراقبت بالینی مربوط به شخص تحت مراقبت	اطلاع‌رسانی اشخاص یا فرایندهای مسئول برای ارائه خدمات مراقبت بهداشتی به شخص تحت مراقبت
۲	ارائه مراقبت فوری به شخص تحت مراقبت	اطلاع‌رسانی اشخاص در صورت نیاز برای ارائه خدمات فوری مراقبت بهداشتی به شخص تحت مراقبت. این امور احتمالاً مستلزم توافق بر سیاست‌هایی است که کاملاً متمایز از سیاست‌های ذکر شده در بخش هدف ۱ است.
۳	پشتیبانی از فعالیت‌های انجام شده از سوی سازمان عرضه کننده خدمات بهداشتی به فرد تحت مراقبت	اطلاع‌رسانی اشخاص یا فرایندها برای توانمندسازی سایر اشخاص برای ارائه خدمات بهداشت و سلامت به فرد تحت مراقبت به‌وسیلهٔ هماهنگ کردن فعالیت‌ها و/یا تجهیزات
۴	توان پرداخت هزینه‌های مراقبتی به شخص تحت مراقبت	اطلاع‌رسانی اشخاص یا فرایندهای مسئول برای اینکه دسترسی به وجوه و/یا مجوز برای بخش پرداخت هزینه خدمات بهداشتی ارائه‌شده به شخص تحت مراقبت را مقدور سازد
۵	مدیریت خدمات بهداشتی و سلامت و تضمین کیفیت	اطلاع‌رسانی اشخاص یا فرآیندهای مسئول برای تعیین دسترس‌پذیری، کیفیت، ایمنی، عدالت و مقرون‌به‌صرفه بودن هزینه خدمات بهداشت و سلامت
۶	آموزش	پشتیبانی از یادگیری و توسعه حرفه‌ای کارشناسان مراقبت بهداشت و درمان
۷	نظارت بهداشت عمومی، واپایش بیماری	اطلاع‌رسانی اشخاص یا فرایندهای مسئول برای پایش جمعیت یا زیرگروه جمعیت برای رویدادهای مهم بهداشت و سلامت و سپس مداخله برای ارائه مراقبت بهداشت و سلامت و یا خدمات مراقبتی پیشگیرانه به افراد مرتبط
۸	فوریت ایمنی عمومی	اطلاع‌رسانی اشخاص مسئول حفظ سلامت و ایمنی عمومی در موقعیتی که برای عموم افراد می‌تواند یک خطر قابل‌توجهی به وجود آورد و احتمالاً نیاز به سیاست‌های متمایز از سیاست‌های بند ۷ است.
۹	مدیریت بهداشت و سلامت جمعیت	اطلاع‌رسانی اشخاص یا فرآیندهای مسئول برای نظارت بر جمعیت یا زیرگروه جمعیت برای رویدادهای سلامت، روندها یا دستاوردها به‌منظور اعمال سیاست یا راهبرد مربوط
۱۰	تحقیق	پشتیبانی از کسب دانش تعمیم‌یافته
۱۱	تحقیقات بازار	پشتیبانی از تهیه محصول یا کسب دانش خاص سازمانی

1- Purpose classification

کد	اصطلاحات رده‌بندی	توضیح (اطلاعاتی)
۱۲	رویه قانونی	اطلاع‌رسانی اشخاص یا فرآیندهای مسئول اجرای قانون، یا اشخاصی که قانوناً موظف به رسیدگی به تحقیقات جنایی، جرائم مدنی، یا تحقیقات نظارتی است.
۱۳	کاربرد برای شخص تحت مراقبت	اطلاع‌رسانی شخص تحت مراقبت و یا نماینده قانونی وی به‌منظور حمایت و پشتیبانی از منافع شخص تحت مراقبت و یا در مورد متوفی در خصوص حمایت از مراقبت از اعضای خانواده
۱۴	نامشخص	افشاء بر اساس مجوز نیاز نیست، یک هدف که اعلام خواهد شد و یا اهدافی که در سایر رده‌ها صدق نمی‌کند.

مبنای منطقی: این فیلد امکان ارزیابی سازگاری و انطباق رویدادهای ممیزی شده با سیاست دسترسی سازمان را فراهم می‌کند.

۷-۴ شناسایی نقطه دسترسی[1]

۷-۴-۱ کد نوع نقطه دسترسی شبکه[2]

توضیح: شناسه نوع نقطه دسترسی شبکه که رویداد ممیزی را مشخص می‌کند.

گزینهٔ انتخابی: اختیاری

قالب /مقادیر: برشماری مانند آنچه در جدول ۱۰ نشان داده شده است، تعیین می‌شود.

جدول ۱۰- کدهای نوع نقطه دسترسی[3]

مقدار	معنی
۱	نام ماشین، شامل نام DNS
۲	نشانی IP
۳	شماره تلفن

1 - Access point identification
2 - Network access point type code
3 - Access point type codes

مبنای منطقی: این مأخذ[1] نوع شناسه نقطه دسترسی به افزاره کاربر را برای بررسی رویداد ممیزی خاص شناسایی می‌کند. این، یک مقدار اختیاری است که ممکن است برای برخی رویدادهای ثبت شده در کارسازهای مجزا به کار رود و طبق نوع نقطه دسترسی شبکه به تحلیل دسترسی کمک کند.

۷-۴-۲ شناسه نقطه دسترسی به شبکه[2]

توضیح: شناسه نقطه دسترسی شبکه کاربر برای رویداد ممیزی. این می‌تواند یک شناسه افزاره، نشانی IP یا سایر شناسه‌های مربوط به یک افزاره باشد.

گزینهٔ انتخابی: اختیاری

قالب/مقادیر: متن ممکن است تنها به مقادیر معتبر برای نوع نقطه دسترسی شبکه معلوم محدود شود. در این صورت، توصیه می‌شود، آنجاکه چند گزینه قابل‌دسترس است تا حد امکان مشخص باشد.

مبنای منطقی: این شناسهٔ مأخذ، نقطه دسترسی شبکه کاربر را شناسایی می‌کند. درنتیجه ممکن است متمایز از کارسازی باشد که عمل در آن انجام شده است. این، یک مقدار اختیاری است که ممکن است در خصوص برخی رویدادهای گروهی به کار رود که در کارسازهای مجزا ثبت شده و به تحلیل داده‌های ثبت شده در کل شبکه کارسازها کمک می‌نمایند.

یادآوری- شناسه نقطه دسترسی شبکه، یک جایگزین برای پاسخگویی شخصی نیست. نشانی‌های IP اینترنت مخصوصاً IPهای نامشخص می‌توانند در یک بازه زمانی کوتاه به بیش از یک شخص اختصاص داده شوند.

مثال ۱:

شناسه نقطه دسترسی شبکه: ۱۹۲.۰.۲.۲

کد نوع نقطه دسترسی شبکه: ۲= نشانی IP

مثال ۲:

شناسه نقطه دسترسی شبکه:۶۱۰-۵۵۵-۱۲۱۲

کد نوع نقطه دسترسی شبکه: ۳= شماره تلفن

۷-۵ شناسایی منبع ممیزی

۷-۵-۱ مرور کلی

داده‌های روند ممیزی می‌تواند از منابع مختلف گردآوری شود، مانند:

- داده‌های امنیتی سامانه‌های اطلاعاتی

1 - Datum
2 - Network access point ID

- خدمات فهرست راهنما
- خدمات تعریف سیاست دسترسی
- داده‌های دسترسی سطح برنامه کاربردی

برای به دست آوردن این داده‌ها، خدمات امنیتی موردنیاز است.

داده‌های ذیل ابتدا برای فرآیندها و سامانه‌های کاربردی موردنیاز می‌باشند. ازآنجایی‌که در برنامه‌های چندلایه، توزیع‌شده یا مرکب منبع شناسایی واضح و مشخص نیست؛ این مجموعه از فیلدها ممکن است برای هر فرایند یا برنامه کاربردی فعال، در رویداد تکرار شود. به‌طور مثال مجموعه‌های مقادیر چندگانه می‌توانند کارسازهای مشارکتی[1] وب، فرایندهای برنامه‌های کاربردی، رشته‌های[2] کارساز پایگاه داده در برنامه کاربردی توزیع‌شده چندلایه را شناسایی کنند. شرکت‌کنندگان رویداد غیرفعال، مانند انتقالات شبکه سطح پایین نیازی به شناسایی ندارند.

بسته به راهبردهای اجرا شده، این احتمال وجود دارد که اجزای برنامه‌های کاربردی مرکب یا توزیع‌شده و چندلایه بیش از یک سابقه ممیزی را برای یک رویداد برنامه کاربردی واحد، تولید کنند. داده‌های مختلف در سابقه ممیزی ممکن است برای تعیین مواردی مانند کاهش داده‌های متوالی پشتیبان مورد استفاده قرار گیرند. این سند پیش‌بینی می‌کند که سازوکارهای گزارش‌دهی و مخزن ذخیره اطلاعات، در صورت نیاز داده را کاهش داده اما سازوکارها را مشخص نمی‌نماید.

۷-۵-۲ ممیزی شناسه محل سازمان[3]

توضیح: موقعیت منبع منطقی در شبکه سازمان مراقبت بهداشتی، به‌طور مثال موقعیت بیمارستان یا سایر مراکز ارائه‌کننده خدمات در گروهی از ارائه‌کنندگان خدمات چند موجودیتی.

گزینهٔ انتخابی: اجباری شرطی

قالب/مقادیر: رشته متن شناسه منحصربه‌فرد در سازمان مراقبت بهداشتی. زمانی که سامانه ممیزی به‌صورت منحصربه‌فرد توسط شناسه منبع ممیزی شناسایی شود، اختیاری است.

مبنای منطقی: این مقدار در میان مکان‌هایی که در یک سامانه اطلاعاتی مربوط به سازمان مراقبت بهداشتی با چند مکان، وجود دارند، تمایز ایجاد می‌کند.

یادآوری- این مقدار توسط برنامه کاربردی که سابقه ممیزی را تولید می‌کند، تعریف می‌شود و حاوی کد منحصربه‌فردی است که سازمان کسب‌وکار (که داده‌ها متعلق به آن است) و سازمان مراقبت بهداشتی آن را می‌شناسد، شناسایی می‌نماید. علاوه بر این، این مقدار، شناسه منبع ممیزی را نیز مشخص و رفع ابهام می‌نماید. مقادیر بسته به نوع کسب‌وکار می‌توانند متفاوت باشند. به عبارتی ممکن است سطوحی از تمایز در سازمان وجود داشته باشد.

1 - web servers
2 - Threads
3 - Audit enterprise site ID

۷-۵-۳ شناسه منبع ممیزی[1]

توضیح: شناسه منبعی که رویداد در آن به وقوع پیوسته است.

گزینهٔ انتخابی: اجباری

قالب/مقادیر: رشته متن شناسه‌ی منحصربه‌فردی که حداقل در شناسه محل سازمان ممیزی وجود دارد.

مبنای منطقی: این فیلد، رویداد را به سامانه منبع مشخص مرتبط می‌سازد. از آن ممکن است، برای گروه‌بندی رویدادها برای تحلیل آن‌ها بر اساس مکانی که رویداد به وقوع پیوسته است، استفاده شود.

۷-۵-۴ کد نوع منبع ممیزی[2]

توضیح: کد نوع منبعی که رویداد در آن به وقوع پیوسته است را مشخص می‌نماید.

گزینهٔ انتخابی: اختیاری

قالب/مقادیر: برشماری مقدار کدگذاری شده، به‌طور اختیاری توسط مجریان سامانه یا به‌عنوان مرجعی از واژگان استاندارد تعریف می‌شود. در غیر این صورت مقادیر پیش‌فرض برای صفات کد، مانند آنچه در جدول ۱۱ درج شده است داده می‌شود.

جدول ۱۱- کدهای نوع منبع ممیزی

مقدار	معنی
۱	واسط کاربر نهایی
۲	افزاره یا تجهیزات کسب داده
۳	فرآیند کارساز وب در سامانه چندلایه
۴	فرآیند کارساز برنامه کاربردی در سامانه چندلایه
۵	فرآیند کارساز پایگاه داده در سامانه چندلایه
۶	کارساز امنیتی، به‌طور مثال واپایش کننده دامنه
۷	اجزاء شبکه در سطح ۳-۱ ایزو
۸	نرم‌افزار عامل در سطح ۶-۴ ایزو
۹	منبع خارجی، نوع نامشخص یا سایر منابع

1 - Audit source ID
2 - Audit source type code

طرح‌وارهٔ XML در RFC 3881 صفات اختیاری را برای کدهای تعریف شده در اجرا یا مراجعه شده به استانداردها، تعریف می‌کند. این صفات در جدول ۱۲، آورده شده است.

جدول ۱۲- صفات مرجع نوع منبع ممیزی

صفت	مقدار
CodeSystem	مرجع OID
CodeSystemName	نام سامانه کدگذاری، به شدت توصیه می‌شود که برای مجموعه کد به‌صورت محلی تعریف‌شده و ارزش‌گذاری شود
DisplayName	ارزش به‌کاررفته در گزارش‌ها و نمایش‌ها
OriginalText	مقدار ورودی که به کد تبدیل شده است

ازآنجاکه منابع ممیزی ممکن است با بیش از یک روش طبقه‌بندی شوند، لذا این امکان وجود دارد که چندین مقدار مشخص شوند.

مبنای منطقی: این فیلد نشان می‌دهد که چه نوعی از منبع توسط شناسه منبع ممیزی تعیین می‌شود. همچنین مقدار اختیاری است که ممکن است برای گروه‌بندی رویدادها به‌منظور تحلیل آن‌ها بر اساس نوع منبعی که رویداد در آن به وقوع پیوسته است، به کار برده شود.

۷-۶ شناسایی شیء شرکت‌کننده

۷-۶-۱ مرور کلی

اشیاء یک رویداد قابل ممیزی به‌عنوان اشیاء شرکت‌کننده اطلاق می‌شوند. داده‌های ذیل با ارائه نمونه‌هایی از اشیاء یا داده‌هایی که به دست آمده‌اند، به فرایند ممیزی کمک می‌کند.

این داده‌ها موردنیاز می‌باشند، مگر درصورتی‌که مقادیر شناسایی رویداد شامل شناسایی شرکت‌کننده فعال و شناسایی منبع ممیزی برای مستندسازی کل رویداد به‌طور کافی قابل ممیزی باشند. سوابق ممیزی تولید که حاوی این داده‌ها هستند، آن‌گونه که در سیاست مراقبت بهداشتی و الزامات قانونی سازمان تعیین شده است، ممکن است غیرفعال و یا فعال شوند.

ازآنجایی‌که رویدادها ممکن است بیش از یک شیء شرکت‌کننده داشته باشند؛ این گروه می‌تواند مجموعه تکراری از مقادیر باشد، به‌طور مثال بسته به سیاست‌های سازمانی و گزینه‌های اجرا خواهیم داشت:

- دو مجموعه مقدار از شیء شرکت‌کننده، می‌توانند در شناسایی دسترسی به اطلاعات شخصی بهداشتی با استفاده از شماره سابقه پزشکی به اضافه رویدادهای خاص در زمینه مراقبت بهداشتی برای شخص تحت مراقبت به کار برده شوند.
- شخص تحت مراقبت و نماینده مجاز او ممکن است با هم شناسایی شوند.
- پزشک حاضر و مشاوره مربوطه ممکن است با هم شناسایی شوند.
- کلیه اشخاص تحت مراقبت که در فهرست کار مشخص شده‌اند، ممکن است شناسایی شوند.

در برخی از موارد، (به‌طور مثال در تحقیقات رادیولوژیکی یا انتقال مقادیر حجیمی از داده‌های رایج HL7 در اسناد)، مجموعه‌ای از اشیاء شرکت‌کننده مربوطه که از طریق شماره ورود یا شماره تحقیق تشخیص داده می‌شوند، شناسایی می‌گردند. توجه شود که هر سابقه ممیزی تنها یک نمونه از ارتباطات هدف مشارکت‌کننده را مستند می‌کند و کلیه ارتباطات حاضر و محتمل را مستند نمی‌کند.

۷-۶-۲ کد نوع شیء شرکت‌کننده[1]

توضیح: کد نوع شیء شرکت‌کننده ممیزی می‌شود. این مقدار متمایز از نقش کاربر یا هرگونه ارتباط کاربر با شیء شرکت‌کننده است.

گزینهٔ انتخابی: اجباری

قالب/مقادیر: برشماری مانند آنچه در جدول ۱۳ نشان داده شده است، تعیین می‌شود.

جدول ۱۳- کدهای نوع هدف شرکت‌کننده

مقدار	معنی
۱	شخص
۲	هدف سامانه
۳	سازمان
۴	سایر موارد

مبنای منطقی: به‌منظور توصیف شیء ذکر شده و نیز پرس‌وجوی فاعل عمل در یک رویداد قابل ممیزی و همچنین ایجاد امکان پرس‌وجو در نوع شیء دارای اهمیت است.

1 - Participant object type code

۷-۶-۳ کد نقش نوع شیء شرکت‌کننده[1]

توضیح: کد، نقش برنامه کاربردی از شیء ممیزی شده شرکت‌کننده را نشان می‌دهد

گزینهٔ انتخابی: اجباری

قالب/مقادیر: برشماری مربوط به کد نوع شیء شرکت‌کننده در جدول ۱۴، نشان داده شده است.

جدول ۱۴- کدهای نقش شیء شرکت‌کننده[2]

مقدار	معنی	کدهای نوع شیء شرکت‌کننده
۱	شخص تحت مراقبت	۱- شخص
۲	موقعیت	۳- سازمان
۳	بخش HER	۲- شیء سامانه
۴	منبع	۱ – شخص ۳- سازمان
۵	فایل اصلی	۲ – شیء سامانه
۶	کاربر	۱ – شخص ۲- شیء سامانه (کاربر غیرانسانی)
۷	لیست	۲- شیء سامانه
۸	کارشناس بهداشت	۱– شخص
۹	تصدیق‌کننده[3]	۳- سازمان
۱۰	ضامن[4]	۱– شخص ۳- سازمان
۱۱	موجودیت کاربر امنیتی	۱– شخص ۲- شیء سامانه
۱۲	گروه کاربر امنیتی	۲– شیء سامانه
۱۳	منبع امنیتی	۲– شیء سامانه
۱۴	تعریف خوشه‌بندی امنیتی	۲ – شیء سامانه
۱۵	ارائه‌کننده	۱– شخص ۳– سازمان
۱۶	مقصد داده	۲- شیء سامانه
۱۷	مخزن ذخیره اطلاعات	۲– شیء سامانه
۱۸	برنامه زمان‌بندی	۲– شیء سامانه

1 - Participant object type code role
2 - Participant object role codes
3 - Subscriber
4 - Guarantor

مقدار	معنی	کدهای نوع شیء شرکت‌کننده
۱۹	مشتری	۳– سازمان
۲۰	شغل	۲- شیء سامانه
۲۱	جریان شغل	۲- شیء سامانه
۲۲	جدول	۲– شیء سامانه
۲۳	معیار مسیریابی	۲– شیء سامانه
۲۴	پرس‌وجو	۲– شیء سامانه

«منبع امنیتی»، یک شیء انتزاعی امنیتی است، به‌طور مثال واسط، صفحه نمایشگر، سند، برنامه و غیره یا حتی سیاهه ممیزی یا مخزن ذخیره اطلاعات.

مبنای منطقی: در مواردی برای تحلیل تفصیلی ممیزی، نمایش خوشه‌بندی‌شده از نوع مشارکت‌کننده با توجه به نقش کاربردی که ایفا می‌نماید، ضرورت دارد.

۷-۶-۴ چرخه عمر داده شیء شرکت‌کننده[1]

توضیح: شناسه مرحله چرخه عمر داده برای شیء شرکت‌کننده. این شناسه می‌تواند برای ارائه روند ممیزی برای داده در طی زمان، به ترتیبی که از سامانه عبور می‌کنند، به کار رود.

گزینهٔ انتخابی: اختیاری

قالب/مقادیر: برشماری مانند آنچه در جدول ۱۵، نشان داده شده است.

جدول ۱۵- کدهای مرحله هدف شرکت‌کننده

مقدار	معنی
۱	ایجاد/ابتکار
۲	واردکردن/رونوشت از اصل
۳	تصحیح
۴	تصدیق
۵	ترجمه
۶	دسترسی/استفاده
۷	عدم شناسایی
۸	یکپارچه‌سازی، خلاصه کردن و استخراج
۹	گزارش
۱۰	صدور/رونوشت

1 - Participant object data life cycle

مقدار	معنی
۱۱	افشاء
۱۲	دریافت افشاء
۱۳	بایگانی
۱۴	حذف منطقی
۱۵	پاک شدن دائمی/خرابی فیزیکی
۱۶	دسته‌بندی مجدد

مبنای منطقی: سیاست‌های سازمانی در امنیت و حریم خصوصی ممکن است مشمول قوانین پاسخگویی متفاوتی بر مبنای چرخه عمر داده باشند. این امر، مقدار متمایزی به آن‌ها می‌دهد.

۷-۶-۵ کد نوع شناسه شیء شرکت‌کننده[1]

توضیح: شناسه‌ای را که در شناسه شیء شرکت‌کننده است، شرح می‌دهد.

گزینهٔ انتخابی: اجباری

قالب/مقادیر: برشماری مقدار کدگذاری شده برای کد نوع شیء مشارکت‌کننده، با استفاده از نام صفت «کد». مجموعه پیش‌فرض این کدها در جدول ۱۶، آورده شده است.

جدول ۱۶- کدهای نوع شناسه هدف شرکت‌کننده

مقدار	معنی	کدهای نوع هدف شرکت‌کننده
۱	شناسه سابقه پزشکی	۱- شخص
۲	شناسه شخص تحت مراقبت	۱- شخص
۳	شناسه واقعه	۱– شخص
۴	شناسه ثبت‌نام بیمه	۱- شخص
۵	شناسه شخصی ملی برای خدمات مراقبت بهداشت (به‌طور مثال، شماره تأمین اجتماعی)	۱ – شخص
۶	شناسه حساب کاربری	۱- شخص ۳- سازمان
۷	شناسه ضامن	۱– شخص ۳– سازمان
۸	نام گزارش	۲- شیء سامانه

[1] - Participant object ID type code

مقدار	معنی	کدهای نوع هدف شرکت‌کننده
۹	شناسه گزارش	۲- شیء سامانه
۱۰	معیار جستجو	۲- شیء سامانه
۱۱	شناسه کاربر سامانه	۱- شخص ۲- شیء سامانه
۱۲	شناسه منبع یکپارچه (URI)	۲- شیء سامانه
۱۳	شناسه شیء (به‌طور مثال شناسه سابقه، آزمایشگاه و غیره)	۲ شیء سامانه

شناسه کاربر و رشته‌های متنِ URI [RFC2396] برای مدیریت امنیت رویدادهای رخداده در شناسایی اشیاء ذکر شده، به کار می‌رود.

کدها ممکن است مجموعه پیش‌فرض بالا باشند، کدهای تعریف شده در اجرا باشند و یا تعیین شماره با مراجعه به مرجع واژگان استاندارد مانند HL7، نسخه 2.4 جدول ۲۰۷، یا انواع تعیین شده در استاندارد ISO 12052 (DICOM) [۱] انجام شود.

طرح‌وارهٔ XML در RFC3881 صفات اختیاری را که در جدول ۱۷ آورده شده است، برای کدهای تعریف شده در اجرا یا مراجعه شده به استانداردها، تعریف می‌نماید.

جدول ۱۷- صفات مرجع کد شناسه شیء شرکت‌کننده[1]

صفت	مقدار
سامانه کد	مرجع OID
نام سامانه کد	نام سامانه کدگذاری، به شدت توصیه می‌شود که برای مجموعه کد به‌صورت محلی تعریف شده و ارزش‌گذاری شود
نام نمایش	مقدار به‌کاررفته در گزارش‌ها و نمایش‌ها
متن اصلی	مقدار ورودی که به کد تبدیل شده است

مبنای منطقی: برای تشخیص در بین شناسه‌های مختلف که ممکن است هر دو یک شیء شرکت‌کننده را شناسایی کنند، موردنیاز است.

1 - Participant object ID code reference attributes

۷-۶-۶ مجموعه سیاست مجوز شیء شرکت‌کننده[1]

توضیح: اشاره به سیاست‌هایی است که دسترسی به شناسه شیء شرکت‌کننده را واپایش می‌کنند.

گزینهٔ انتخابی: اختیاری

قالب/مقادیر: ارزش‌ها، رشته‌های متن تعریف‌شدهٔ اجرا و سازمان است.

۷-۶-۷ حساسیت شیء شرکت‌کننده[2]

توضیح: حساسیت تعریف سیاست برای شناسه شیء شرکت‌کننده را مشخص می‌کند، مانند وضعیت VIP، HIV، بهداشت روانی و موضوعات مشابه.

گزینهٔ انتخابی: اختیاری

قالب/مقادیر: رشته‌های متن تعریف‌شده سازمان و اجرا هستند.

۷-۶-۸ شناسه شیء شرکت‌کننده[3]

توضیح: نمونه ویژه‌ای از شیء شرکت‌کننده را شناسایی می‌کند.

گزینهٔ انتخابی: اجباری

قالب/مقادیر: رشته متن. قالب مقدار به کد نوع شیء شرکت‌کننده و کد نوع شناسه شیء شرکت‌کننده وابسته است.

مبنای منطقی: این فیلد، نمونه ویژه‌ای از شیء را شناسایی می‌کند، به‌طور مثال شخص تحت مراقبت را تعیین می‌نماید تا مسائل امنیتی و حفظ محرمانگی را تشخیص دهد/ پیگیری کند.

یادآوری- ملاحظه شود که این فیلد، کلید شناسه منحصربه‌فرد اولیه برای شیء است؛ بنابراین می‌تواند فیلد داده مرکب باشد.

۷-۶-۹ نام شیء شرکت‌کننده[4]

توضیح: نمونه توصیف‌گر ویژه در شناسه شیء شرکت‌کننده ممیزی شده، مانند نام یک شخص.

گزینهٔ انتخابی: اختیاری

قالب/مقادیر: رشته متن

---

1 - Participant object Permission PolicySet
2 - Participant object sensitivity
3 - Participant object ID
4 - Participant object name

مبنای منطقی: این فیلد ممکن است برای پرس‌وجو/گزارش در شناسایی رویدادهای ممیزی برای شخص خاصی به کار برده شود، به‌طور مثال در شناسه‌های شیء شرکت‌کننده یکسان چندگانه (شناسه شخص تحت مراقبت، شناسه سابقه پزشکی، شناسه واقعه).

۷-۶-۱۰ پرس‌وجوی شیء شرکت‌کننده[1]

توضیح: پرس‌وجوی واقعی برای شیء شرکت‌کننده

گزینهٔ انتخابی: اختیاری

قالب/مقادیر: داده کدگذاری شده ۶۴ بیتی

مبنای منطقی: به دست آوردن ورودی پرس‌وجو در فرایند پرس‌وجو برای شناسایی رویداد خاص، می‌تواند در پرس‌وجوی رویدادها ضرورت داشته باشد. با توجه به تمایزهای موجود میان اجراهای پرس‌وجو و کدگذاری داده برای آنها، داده‌ها در بسته‌های کدگذاری شده‌ی ۶۴ بیتی هستند، متعاقباً این داده‌ها ممکن است توسط فرایند تحلیل ممیزی پایین به بالا کدگشایی یا تفسیر شوند.

۷-۶-۱۱ جزئیات شیء شرکت‌کننده[2]

توضیح: داده‌های تعریف‌شده در اجرا که در ارتباط با جزئیات خاصی از شیء به‌دست‌آمده یا به‌کاررفته هستند.

گزینهٔ انتخابی: اختیاری

قالب: جفت نوع و مقدار. صفت «نوع»، رشته متن تعریف‌شده در اجرا است. صفت «مقدار»، یک داده کدگذاری شده‌ی ۶۴ بیتی است.

مبنای منطقی: مقادیر یا جزئیات خاص از شیء دست آمده ممکن است برای اجراهای ممیزی خاصی مطلوب باشند. ارزش نوع جفت امکان استفاده از مقادیر و شناسه نوع شیء توسعه‌پذیر محلی و تعریف شده در اجرا مقدور می‌سازد. به‌طور مثال، شیء یک تشخیص بالینی ممکن است حاوی چند نتیجه آزمایش باشد؛ در این صورت این عنصر می‌تواند نوع و شماره و نوع نتایج را مستند کند.

بسیاری از روش‌های کدگذاری برای این عناصر مقدور هستند؛ بنابراین، مقدار، داده کدگذاری شده ۶۴ بیتی است. متعاقباً این داده‌ها ممکن است توسط فرایند تحلیل ممیزی پایین به بالا کدگشایی یا تفسیر شوند.

1 - Participant object query
2 - Participant object detail

۸ سوابق ممیزی برای رویدادهای فردی

۸-۱ رویدادهای دسترسی[1]

همان‌طور که در جدول ۱۸ نشان داده شده است، این سابقه ممیزی ایجاد، مطالعه، تغییر و حذف اطلاعات بهداشت شخصی را شرح می‌دهد.

جدول ۱۸- قالب سابقه ممیزی برای رویدادهای دسترسی

دسته	نام فیلد	گزینه	کاهش مقادیر
رویداد مربوط	EventID	M	شناسه رویداد ممیزی
	EventActionCode	M	عمل انجام شده در رویداد که سیاهه ممیزی را ایجاد می‌کند. مقدار زیر تنظیم می‌شود: EV:"C" (Create) "R"(Read) "U"(Update) "D"(Delete)
	EventDateTime	M	زمان/روز وقوع رویداد
	EventOutcomeIndicator	U	کد موفقیت (یا شکست) رویداد
	EventTypeCode	U	نوع رویداد
کاربر مربوط (۱..۲)	UserID	M	شناسه فرد یا فرآیند عملیاتی داده. درصورتی‌که هم فرد و هم فرایند مشخص باشند، هر دو را شامل می‌شود. این ارزش، مقدار منحصربه‌فرد در منبع ممیزی است (شناسه منبع ممیزی)
	AlternateUserID	U	شناسه جایگزین فرد یا فرآیند عملیاتی داده
	UserName	U	نام فرد یا فرآیند عملیاتی داده
	UserIsRequestor	U	ارزش نشان می‌دهد که آیا فرد یا فرآیند عملیاتی داده، درخواست‌کننده این رویداد باشد یا نه. مقدار زیر تنظیم می‌شود: EV TRUE
	RoleIDCode	U	نقش فرد یا فرآیند عملیاتی داده در رویداد
	PurposeOfUse	U	این کد هدف از کاربرد داده در دسترس را نشان می‌دهد.
	NetworkAccessPointTypeCode	U	کد نوع نقطه دسترسی به شبکه
	NetworkAccessPointID	U	شناسه نقطه دسترسی به شبکه
سامانه	AuditEnterpriseSiteID	U	موقعیت منطقی سامانه منبع واقعه مورداستفاده

1 - Access events

دسته	نام فیلد	گزینه	کاهش مقادیر
منبع واقعه مربوط (۱)			برای تغییر AuditSourceID
	AuditSourceID	M	شناسه منحصربه‌فرد سامانه منبع واقعه
	AuditSourceTypeCode	U	کد نوع سامانه منبع واقعه
شیء شرکت‌کننده مربوط (اطلاعات بیمار) (۱)	ParticipantObjectTypeCode	M	کد نوع شیء شرکت‌کننده. مقدار زیر تنظیم می‌شود: EV1 (فرد)
	ParticipantObjectTypeCodeRole	M	کد نقش شیء شرکت‌کننده. مقدار زیر تنظیم می‌شود: EV1 (بیمار)
	ParticipantObjectDataLifeCycle	U	شناسه مرحله چرخه عمر شیء شرکت‌کننده
	ParticipantObjectIDTypeCode	M	کد نوعی که کل حاوی شناسه شیء شرکت‌کننده است. مقدار زیر تنظیم می‌شود: EV2 (شناسه بیمار)
	ParticipantObjectPolicySet	U	مجموعه سیاست مجوز برای شناسه شیء شرکت‌کننده، به‌طور مثال اطلاعات رضایت بیمار
	ParticipantObjectSensitivity	U	حساسیتی که سیاست برای شناسه شیء شرکت‌کننده تعریف کند.
	ParticipantObjectID	M	شناسه نمونه‌ای از شیء شرکت‌کننده شناسه بیمار تنظیم می‌شود.
	ParticipantObjectName	U	نام شیء شرکت‌کننده. نام شخص تحت مراقبت تنظیم می‌شود.
	ParticipantObjectDetail	U	جزئیات نمونه شیء شرکت‌کننده
شیء شرکت‌کننده مربوط (اطلاعات به‌دست‌آمده از بخش EHR) (1..N)	ParticipantObjectTypeCode	M	مقدار به‌صورت زیر تنظیم می‌شود: EV2 (هدف سامانه)
	ParticipantObjectTypeCodeRole	M	کد نقش شیء شرکت‌کننده. مقدار به‌صورت زیر تنظیم می‌شود: EV3 (بخشEHR)
	ParticipantObjectDataLifeCycle	U	شناسه مرحله چرخه عمر داده هدف شرکت‌کننده
	ParticipantObjectIDTypeCode	M	کد نوعی که در شناسه شیء شرکت‌کننده است. مقدار به‌صورت زیر تنظیم می‌شود: EV13(شناسه شیء)
	ParticipantObjectPolicySet	U	مجموعه سیاست مجوز برای شیء شرکت‌کننده
	ParticipantObjectSensitivity	U	حساسیتی که سیاست برای شناسه شیء شرکت‌کننده تعریف می‌کند.

دسته	نام فیلد	گزینه	کاهش مقادیر
	ParticipantObjectID	M	شناسه نمونه از شیء شرکت‌کننده. شناسه بخش EHR تنظیم می‌شود.
	ParticipantObjectName	U	نام شیء شرکت‌کننده نام بخش EHR تنظیم می‌شود.
	ParticipantObjectDetail	U	جزئیات نمونه شیء شرکت‌کننده

۸-۲ رویدادهای پرس‌وجو[1]

در این سابقه ممیزی که در جدول ۱۹ آورده شده است، رویداد یک پرس‌وجوی فرستاده‌شده یا دریافت شده شرح داده می‌شود. پاسخ به پرس‌وجو ثبت نمی‌شود؛ اما به‌ندرت واقعیتی که پرس‌وجو فرستاده شده است، ثبت می‌گردد.

جدول ۱۹- قالب سابقه ممیزی رویدادهای پرس‌وجو[2]

طبقه	نام فیلد	گزینه	محدودیت مقادیر
مرتبط با رویداد	EventID	M	شناسه رویداد ممیزی
	EventActionCode	M	عمل انجام‌شده در رویداد که سیاهه ممیزی را تولید می‌کند. مقدار زیر تنظیم می‌شود: EV "E" (Execute)
	EventDateTime	M	زمان/تاریخ وقوع رویداد
	EventOutcomeIndicator	U	کد موفقیت (یا شکست) رویداد
	EventTypeCode	U	نوع رویداد
مرتبط با پرسشنامه (۱)	UserID	M	داده فرایند عملیاتی. مقدار منحصربه‌فردی در شناسه منبع ممیزی است.
	AlternateUserID	U	شناسه جایگزین فرد یا فرایند عملیاتی داده.
	UserName	U	نام فرایند عملیاتی داده
	UserIsRequestor	U	این مقدار نشان می‌دهد که آیا فرد یا فرایند عملیاتی داده درخواست‌کننده

1 - Query events
2 - Audit record format of query events

طبقه	نام فیلد	گزینه	محدودیت مقادیر
			این رویداد است یا نه.
	RoleIDCode	U	نقش فرد یا فرآیند عملیاتی داده را در این رویداد نشان می‌دهد
	PurposeOfUse	U	این کد هدف از کاربرد داده در دسترس را نشان می‌دهد.
	NetworkAccessPointTypeCode	U	کد نوع نقطه دسترسی به شبکه
	NetworkAccessPointID	U	شناسه نقطه دسترسی به شبکه
مرتبط با پرسش رو به جلوی (۱)	UserID	M	شناسه فرایندی که به پرس‌وجو پاسخ می‌دهد. ارزش منحصربه‌فردی در منبع ممیزی است (Audit-SourceID)
	AlternateUserID	U	شناسه جایگزینِ فرایند که به پرس‌وجو پاسخ می‌دهد
	UserName	U	نام فرایندی که به پرس‌وجو پاسخ می‌دهد
	UserIsRequestor	U	این مقدار نشان می‌دهد که آیا فرایندی که به پرس‌وجو پاسخ می‌دهد درخواست‌کننده است یا نه.
	RoleIDCode	U	کد نقش فرایندی که در زمان اجرا بر روی داده عملیات انجام می‌دهد.
	NetworkAccessPointTypeCode	U	کد نوع نقطه دسترسی شبکه
	NetworkAccessPointTypeCode	U	شناسه نقطه دسترسی شبکه
مرتبط با شرکت‌کننده جایگزین (N..0)	UserID	M	شناسه شرکت‌کننده که مربوط و شناخته شده است. به‌ویژه فرد یا فرایندی که درخواست‌کننده است. مقدار منحصربه‌فردی در منبع ممیزی است. (Audit-SourceID)
	AlternateUserID	U	شناسه جایگزینِ شرکت‌کننده جایگزین
	UserName	U	نام جایگزینِ شرکت‌کننده جایگزین
	UserIsRequestor	U	این مقدار نشان می‌دهد که آیا شرکت‌کننده جایگزین درخواست‌کننده این رویداد است یا نه.
	RoleIDCode	U	نقش شرکت‌کننده جایگزین

طبقه	نام فیلد	گزینه	محدودیت مقادیر
	NetworkAccessPointTypeCode	U	نوع نقطه دسترسی به شبکه
	NetworkAccessPointID	U	شناسه نقطه دسترسی به شبکه
مرتبط با سامانه منبع واقعه (۱)	AuditEnterpriseSiteID	U	مکان منطقی سامانه‌ی منبع واقعه. برای تغییر شناسه منبع ممیزی به کار می‌رود.
	AuditSourceID	M	شناسه منحصربه‌فرد سامانه‌ی منبع واقعه
	AuditSourceTypeCode	U	کد نوع سامانه منبع واقعه
مرتبط با شیء شرکت‌کننده (محتویات پرس‌وجو) (۱)	ParticipantObjectTypeCode	M	کد نوع شیء شرکت‌کننده مقدار زیر تنظیم می‌شود: EV2 (سامانه)
	ParticipantObjectTypeCodeRole	M	کد نقش شیء شرکت‌کننده. مقدار زیر تنظیم می‌شود: EV3 (گزارش)
	ParticipantObjectDataLifeCycle	U	شناسه مرحله چرخه عمر شیء شرکت‌کننده
	ParticipantObjectIDTypeCode	M	این کد نوع حاوی شناسه شیء شرکت‌کننده است. مقدار زیر تنظیم می‌شود: EV 10 (قاعده پرس‌وجو)
	ParticipantObjectPolicySet	U	مجموعه سیاست مجوز برای شناسه شیء شرکت‌کننده
	ParticipantObjectSensitivity	U	حساسیتی که سیاست برای شناسه شیء شرکت‌کننده تعریف می‌کند.
	ParticipantObjectID	M	شناسه نمونه از شیء شرکت‌کننده
	ParticipantObjectName	U	نام شیء شرکت‌کننده
	ParticipantObjectQuery	M	محتویات پرس‌وجو که در بسته‌های ۶۴ بیتی کد شده است. این محتویات باید توسط توسعه‌دهنده عرضه‌کننده تحلیل شوند.
	ParticipantObjectDetail	U	جزئیات نمونه شیء شرکت‌کننده

۹ مدیریت امنیت ممیزی داده

۹-۱ ملاحظات امنیتی[1]

به‌منظور حفظ محرمانگی و یکپارچگی سوابق سلامت و نیز دسترس‌پذیری به اطلاعات سامانه آن معیارهای ذیل در IETF RFC 3881 آورده شده است.

داده‌های ممیزی باید امنیت حداقلی را برای فعالیت‌ها و داده‌های ممیزی شده داشته باشند که شامل واپایش دسترسی، یکپارچگی داده و عملیات بازیابی است. این سند نیاز به سیاست‌ها و روش‌های فنی را تائید می‌کند، اما آن‌ها را تعیین نمی‌کند.

امکان نامشخص بودن کاربرد داده‌های ممیزی قابل‌قبول است، به‌طور مثال ردیابی تکرار و ماهیت استفاده از سامانه برای ارزیابی بهره‌وری. استاندارد ASTM E2147-01 در بند ۵-۳-۱۰ عنوان می‌کند «در سابقه سامانه اطلاعات بهداشتی، استفاده را به دلایلی غیر از اجبار امنیتی و تشخیص شکاف‌های امنیتی منع کنید، به‌طور مثال ممیزی‌ها برای جستجوی پروفایل فعالیت یا پروفایل جابجایی کارمندان به کار نمی‌روند». [۱۰]

مدیریت سوابق ممیزی باید از استاندارد بین‌المللی مدیریت رکورد در استاندارد ISO 15489-1 تبعیت کنند. [۳] الزامات امنیتی در بایگانی سوابق ممیزی مشابه هستند با آنچه در بایگانی سوابق بهداشت الکترونیک در استاندارد ISO/TS 21547 آورده شده است [۵].

رهنمود[2] بایگانی درازمدت با اطمینان از یکپارچگی داده در سندهای IETFRC 4810 و IETF RFC 4998 ارائه شده است.

بهتر است به امنیت روند ممیزی توزیع‌شده توجه ویژه‌ای شود. سوابق الکترونیک بهداشت، ممکن است در چندین سامانه اطلاعاتی و در دامنه‌هایی که از نظر سیاست امنیتی پراکنده هستند، توزیع شوند؛ که این امر نیز به روند ممیزی مربوط است. امنیت باید در روندهای ممیزی منطقی تأمین شود.

۹-۲ امن کردن دسترس‌پذیری به سامانه ممیزی[3]

سامانه ممیزی باید در زمانی که سامانه اطلاعات بهداشت فعال است، معیارهای کافی برای اطمینان از اینکه ورودی‌ها در روند ممیزی ایجاد می‌شوند فراهم آورد.

سامانه ممیزی باید در زمان ازکارافتادن روند ممیزی، خاموش شدن یا کار نکردن سامانه به دلیل خرابی، کلیه‌ی نمونه‌ها را مستند کند.

سامانه ممیزی باید نشان و یا گزارش دهد که چه ممیزی‌هایی در هر زمانی فعال یا غیرفعال است.

---

1 - Security considerations
2 - Guidance
3 - Securing the availability of the audit system

۹-۳ الزامات نگهداری[1]

سازمانی که مسئول حفظ و نگهداری از سیاهه ممیزی است، باید سیاست امنیتی حاکم بر سوابق امنیتی را تعریف نماید.

در نگهداری سوابق ممیزی باید از الزامات قانونی و سیاست‌های مربوط تبعیت شود.

نگهداری سوابق ممیزی باید طول عمر سوابق سلامت، داده و مستندات را پشتیبانی نماید.

۹-۴ امن کردن محرمانگی و یکپارچگی روندهای ممیزی[2]

سامانه ممیزی باید معیارهای امنیتی کافی را برای حفاظت از سیاهه ممیزی در برابر دستکاری ارائه کند. به‌ویژه، باید

الف- امنیت را در دسترسی به سوابق ممیزی فراهم نماید،

ب- از دسترسی به افزاره‌های ممیزی سامانه حراست کند، تا از سوءاستفاده یا به خطر افتادن آن‌ها جلوگیری شود،

پ- کلیه‌ی فعالیت‌ها با سیاهه امنیتی که در آن زمان، فعالیت و اقدام کننده مشخص است، پیگیری شوند،

ت- در زمانی که روند ممیزی ازکارافتاده است، خاموش است و یا سامانه خراب شده است، کل وقایع مستند شود، و

ث- آنچه ممیزی می‌شود، در هر زمانی، فعال یا غیرفعال گزارش شود.

۹-۵ دسترسی به داده ممیزی[3]

دسترسی به داده ممیزی باید به شدت واپایش شده و خود موضوع ممیزی باشد. دسترسی به روند ممیزی نباید به‌طور مستقیم باشد، بلکه باید از طریق سامانه اطلاعاتی مناسبی صورت گیرد، به‌نحوی‌که واپایش انجام شود.

تجهیزات ممیزی باید تحلیل روند ممیزی در هر کد یا نام فیلد تعریف‌شده‌ای از بند ۷، با هر تاریخ/دوره زمانی، به‌صورت فردی یا گروهی (به‌طور مثال دسترسی کامل با کاربر «X»، حذف کامل رویدادها با کاربران نقش «Y»، کلیه رویدادهای شامل فرد تحت مراقبت «Z» در ماه گذشته و غیره) مهیا کند.

در برخی از موارد، لازم است کاربر ممیزی علاوه بر دسترسی به روند ممیزی به منابع اطلاعات نیز دسترسی داشته باشد، به‌طور مثال دسترسی به الگوها (برای مثال: کلیه جستجوهایی که در مورد اطفال انجام شده، توسط فردی که پزشک مخصوص اطفال نیست یا ارتباطی با پزشک اطفال ندارد).

---

1 - Retention requirements
2 - Securing the confidentiality and integrity of audit trails
3 - Access to audit data

پیوست الف

(اطلاعاتی)

فرانامه‌های ممیزی

الف-۱ مرور کلی

انواع مختلفی از ممیزی وجود دارد: امنیت، حریم خصوصی، مسائل قانونی، تدارکات، کارکرد سامانه، کارکرد شبکه، مدیریت پیکربندی، کشف نفوذ، و غیره. این پیوست فرانامه‌های مختلف مربوط به استفاده از سیاهه‌های ممیزی را شرح می‌دهد.

الف-۲ یک نمونه نارضایتی افراد مشهور

زمانی که یک فرد مشهور در بیمارستان است، فردی از اعضای کارمندان به وضعیت افراد بیمار واقف بوده و از سامانه اطلاعات پرستاری و مراقبت برای یافتن شماره اتاق شخص تحت مراقبت و اطلاعات پرونده بهداشت و سلامت وی استفاده می‌نمایند. سپس اطلاعات را به مجلات و روزنامه‌ها می‌فروشد.

شخص تحت مراقبت تصویر خود را روی جلد یک روزنامهٔ برجسته یافته و به مأمور امنیتی اطلاعات خصوصی بیمارستان شکایت می‌کند. مأمور از سامانه ممیزی استفاده کرده و کل اطلاعات موجود در سوابق بهداشت و سلامت شخص را پویش کرده و به رویداد رخداده خارج از بازه زمان‌بندی‌شده معاینه عمومی پی می‌برد. دو پرستار مسئول مراقبت و بررسی بوده‌اند یکی از آنها اقرار می‌کند که وظیفه‌اش را به‌خوبی انجام نداده و دیگری از این مسئله سرباز می‌زند.

این فرانامه به شدت به سوابق ممیزی و همچنین فرآیند فعالیت ممیزی که ثبت شده، بستگی دارد و باید موارد ذیل را شامل شود:

- ایجاد سابقه /سیاهه ممیزی
- انتقال سابقه /سیاهه ممیزی به داخل مخزن ذخیره اطلاعات (شامل صف‌بندی و ذخیره‌سازی محلی؟)
- دریافت سابقه /سیاهه ممیزی
- ذخیره سابقه /سیاهه ممیزی
- پرس‌وجو/جستجو سیاهه ممیزی و تعیین آنچه رخ داده. این امر مستلزم اقدامات ذیل است:
  - جستجو از طریق قابلیت تاریخ و
  - سامانه‌های ممیزی که دست کم:

- شناسایی کاربری که گزارش شده است به سوابق شخص تحت مراقبت در موضوع داده شده، نگاه کرده است.
- شناسایی هر نمونه کاربر مشخصی که به هر موضوعی در سوابق شخص تحت مراقبت دسترسی دارد و
- شناسایی هر نمونه دسترسی به گره شبکه‌ای یک شخص تحت مراقبت.

- منطبق با استاندارد RFC 3881، برای ایجاد امکان جستجو

- آنجاکه جریان کار رادیولوژی ممیزی می‌شود. منطبق با استاندارد ISO 1252 [۱](DICOM)

فرانامه مذکور برخی نیازهای شخص تحت مراقبت ویژه را تأمین می‌کند:

- مواردی که مهاجم به شدت انگیزه سرقت را دارد، به‌طور مثال فردی که ندانسته در مکانی راه رفته و در جستجوی اطلاعات است.

- قربانی خشونت:

- شخص تحت مراقبت مأمور امنیتی را مطلع می‌کند تا دسترسی به اطلاعات شخصی سلامت را به‌وسیلهٔ برچسب زدن متفاوت نسبت به برچسب‌های مورداستفاده برای شناسایی اتاق‌های VIP، غیرفعال نماید (بخش مدیریت اجرایی ممکن است یک مجموعهٔ استاندارد از برچسب‌ها را برای شناسایی این نوع از داده مربوط به اشخاص داشته باشد). با توجه به سامانه ممیزی، این نمونه نباید ثبت شود، زیرا شخص تحت مراقبت خود قربانی خشونت است، اما ترجیحاً اسم او باید ثبت شده و مأمور امنیتی باید هشدارهای لازم را در این خصوص به شخص دهد. ما می‌خواهیم یک کد برای خشونت را ثبت کنیم، اما به‌وضوح نمی‌توانیم به متن کامل سابقه ممیزی پی ببریم.

با توجه به اصول ممیزی، ما می‌توانیم موارد ذیل را استاندارد نماییم:

- مقوله‌های هشدار امنیتی برای ارسال هشدار امنیتی نیاز به یک طرزکار دارند. ما برای بررسی مزاحمت احتمالی و فعالیت غیرقانونی باید مجهز به سامانه هشدار امنیتی باشیم و هم‌چنین هشدارهای قوی‌تر برای فرانامه‌هایی که در زیر مشخص شده است:

- ما باید دارای کدهایی بوده و به برنامه برای کشف الگو اطمینان داشته باشیم.

- ما می‌توانیم یک قابلیت اعمال سیاست داشته باشیم، برای فرایند ممیزی، آنجاکه سیاست تعریف می‌کند جه زمانی و چه چیزی هشدار داده شود.

- نیاز است که از این قابلیت از سیاهه سامانه استفاده شود: ارسال انتخابی از سیاهه‌ها که الگوهای خاص (ساده) را با برنامه مجزا که بخشی از خدمت ممیزی اساسی نیست، تطبیق می‌دهند. این برنامهٔ «بیننده» دیگر، در جستجوی رفتار بد و ارسال هشدار است (این نوع برنامه می‌تواند برای مشکلات سخت‌افزاری هم کاربرد داشته باشد).

- قابلیت استخراج داده اولیه از بایگانی ممیزی
- گزینه: یک افزونه برای جستجوهای خاص از مخزن ممیزی اضافه کنید، اما حداقل قابلیت رونوشت‌برداری تمام داده‌های به‌دست‌آمده از پایگاه داده ممیزی را فراهم نمایید، بنابراین، شما می‌توانید تحلیل دستی را در مرحله ۱ انجام دهید.

خدمات اطلاع‌رسانی می‌تواند ساده یا پیچیده باشد، اما ما باید به این مسئله واقف باشیم که چه چیز به کجا ارسال شود. خدمات اطلاع‌رسانی می‌تواند، خدمات وابسته اختیاری باشد. دو تغییر در این مورد وجود دارد که باید به آن توجه شود. این دو تغییر به شرح ذیل است:

موضوعات تحت مراقبت مهم، که نفوذگر انگیزه بالایی برای آنها ندارد.

محیط تهدید اولیه: اشخاصی که نفوذگر روی آنها سرمایه‌گذاری نکرده یا انگیزه نفوذ را ندارد، به‌طور مثال مهاجم وقت زیادی را صرف تطمیع کردن کارمندان داخلی نکرده یا وقت آنها را صرف پرس‌وجو مستقیم در پایگاه داده آنها نمی‌کنند. ما تنها در جستجوی تراکنش‌های عادی نامناسب هستیم. مخزن دادهٔ ممیزی باید قابلیت پرس‌وجو برای دسترسی به‌وسیلهٔ IP، PID، کاربر، بازهٔ زمانی و غیره را دارا باشد.

موضوعات تحت مراقبت مهم، که نفوذگر انگیزه بالایی برای آنها دارد.

مهاجمانی که از قابلیت‌های پرس‌وجو از پایگاه داده‌های زیربنایی استفاده کرده‌اند و فقط از جستجو با توابع مشخص و از طریق رابط کاربری مخزن ذخیره اطلاعات برای به دست آوردن اطلاعات استفاده نکرده‌اند (به‌طور مثال: مدیران اجرایی پایگاه داده).

قابلیت‌های موردنیاز: سیاهه‌های مربوط به پرس و جوی ممیزی به شناسه شخص تحت مراقبت، زمان دستیابی و شناسه کاربر، تحلیل کلی مخزن ذخیره اطلاعات در ارتباط است.

مخزن ممیزی باید توانایی رونوشت‌برداری (به یک خدمت گزارش‌دهی؟). سوابق ممیزی بر مبنای PID، ID سامانه، پنجره تاریخ و غیره را داشته باشد.

خدمت گزارش‌دهی، اطلاعات کدگذاری شده را از مخزن دریافت کرده و گزارش را به هر طریقی که آنها انتخاب کنند، نشان می‌دهد (ترجیحاً یک مورد قابل‌استفاده).

واسط کاربری موردنیاز: (آنجا که مخزن ممیزی باید پیامی مبنی بر اینکه خدمت گزارش‌دهی و خدمت تحلیل قابل‌درک است ارسال کند) (واسط کاریری تهیه شده، نیمهٔ دیگر را تشکیل می‌دهد).

چهار سطح:

الف- رویدادهای مربوط به شخص تحت مراقبت‌های ویژه: برای نمایش هر پرس‌وجویی خود را به زحمت نینداز و تنها زمانی به من بگو که رویدادهای ممیزی مرتبط با داده این شخص وجود دارد.

ب- در مورد پرس‌وجوهایی به من بگو که تو آگاه هستی که ممکن است نتایجی در مورد داده شخص حتی اگر داده شناسه شخص لیست نشده باشد را برمی‌گرداند: پرس‌وجوهای قطعی و عدم حساس به زمان (نظیر پرس‌وجوهای ذخیره‌شده به شکل XDS).

پ- تمام رویدادهای مربوط به شخص را در چند پنجرهٔ استاندارد به من می‌دهد: کاربر، پنجره زمان، نوع رویداد و مجموعه‌ای از سامانه‌های موردعلاقه. سامانه‌های جالب (برای مثال: تمام ورود و خروج‌های به/از سامانه).

ت- پیچیده: پرس‌وجوهای مشتری: پرس‌وجوهای ایزو 12052[۱] (DICOM)، پرس و جوی جریان کار آزمایشگاه که به جریان کار وابسته هستند؛ و لازم است شما حالت پایگاه داده را زمانی که پرس و جوی شما انجام شده است بدانید.

سطوح الف، ب و پ ممکن است از طریق رابط کاربری مستقیم به مخزن ذخیره اطلاعات متصل باشند.

یک خدمت تحلیل ممکن است برای سطح ت به کار رفته و در بالاترین سطوح قرار گیرد.

قابلیت بالقوه: پرس‌وجوهای ممیزی به‌طور دستی یا از طریق سامانه خدمات تحلیل ثبت می‌شود.

زمینه جدید بالقوه برای ممیزی: تحلیل/مقایسه /ارتباط بین جدول زمان‌بندی و اصول ممیزی. تمامی این موارد، امکان دسترسی غیر نرمال یا هماهنگ نشده به اطلاعات را نشان می‌دهد.

خدمات اختیاری: خدمت پرس‌وجو انباره/تحلیل. آیا آنها به روند جستجوی غیرعادی کمک می‌کند؟

الف-۳ نمونه حقوق قانونی اجرایی در خصوص محرمانگی (عطف به ماسبق و غیرفعال)

در این فرانامه، شخص تحت مراقبت نمی‌خواهد همسایه مجاورش که ارائه‌کننده خدمات مراقبت بهداشتی است، از وضعیت سلامت وی آگاهی یابد؛ بنابراین وی ممکن است دستورالعملی به مراقب سلامت اولیه خود مبنی بر مسدود کردن دسترسی همسایه به سابقه مراقبت بهداشتی‌اش صادر نماید. در هفته‌های آتی، مسئول حفظ محرمانگی کلینیک اولیه هشداری درخصوص اقدام همسایه برای دسترسی به سوابق وی و تخطی از سیاست سازمانی و در مقابل جلوگیری از دسترسی وی دریافت می‌کند. متصدی حفظ محرمانگی به شخص تحت مراقبت موضوع اقدام برای دسترسی و عدم موفقیت را اعلام می‌کند.

قابلیت‌های موردنیاز: فهرست دسترسی به سابقه بهداشت با وارد شدن به سامانه توسط پزشک/ کاربر؛ فهرست کردن/نمایش دادن دسترسی‌هایی که با شکست مواجه شده‌اند؛ و هشدارهایی که هنگام آگاهی از رویداد دسترسی غیرمجاز براساس دستورالعمل ارسال می‌شوند.

- در مورد کاربری رخ نمون[1] به‌صورت پایین/بالا نیز نیاز به قابلیت تحلیل ممیزی عطف به ماسبق وجود دارد. «داده‌ها را به من بدهید و من آنها را تحلیل خواهم کرد»

1 - Profile

- این فرانامه تنها زمانی وجود دارد که پیامدهای رویداد شکست/موفقیت و نیازهای ممیزی از طریق PID، قادر به «پرس‌وجو» باشند.

مسائل:

- در دنیای واقعی، نمایش و ذخیره خودکار زیادی از داده‌ها وجود دارد. در اغلب تراکنش‌ها نام شخص تحت مراقبت در داده‌ها نیست؛ درحالی‌که در اطلاعات برنامه کاربردی مربوط وجود دارد. به‌عنوان نمونه: هنگامی‌که برنامه‌ریزی ملاقات افراد صورت می‌پذیرد، داده‌هایشان از قبل بر روی صفحه‌نمایش اتاق معاینه فراخوانی[1] می‌شوند. خدمت ممیزی نیاز به توانایی دارد برای تلفیق و تطبیق اینکه چه کسی وارد اتاق معاینه در زمان برنامه‌ریزی شده است.
- در نمونه بالا در مورد اقدام به دسترسی غیرمجاز توسط ارائه‌کننده خدمت مراقبت بهداشتی همسایه، یا باید پرس‌وجوها از منبع پیش‌بینی‌نشده افشا شوند و یا توسط برنامه کاربردی درک شوند.
- «خدمت ناظر[2]» می‌تواند فهرست سفیدی از اتاق‌های معاینه که می‌توانند داده‌ها را از قبل فراخوانی کرده و آن‌ها را برای اعلام ارسال نمایند، داشته باشد؛ تا به این ترتیب پی ببرد که آیا پرس‌وجوها از منبع پیش بینی نشده ارسال شده است و یا آیا خلاف دستورالعمل رضایت و دسترسی هستند. تعیین آنچه خدمت ناظر اعلام می‌کند و زمان اعلام، موضوع سیاست داخلی است.

الف-۴ نمونه کارساز به خطر افتاده

ثبت‌نام در خدمت بهداشت عمومی جدید اعلام می‌شود و کسی که کارساز را طراحی کرده است در تغییر رمز عبور اهمال کرده است. نفوذگری به‌طور تصادفی به کارساز دسترسی پیدا می‌کند و شروع به بمباران هرزنامه با ثبت‌نام بهداشت عمومی از طریق آن می‌کند. حجم غیر معمولی از رویدادهای ممیزی و دسترسی‌های مدیر از آدرس IP ناشناخته منجر به محرکی برای بررسی سریع سیاهه ممیزی توسط متصدی امنیت و پی بردن به آنچه رخ می‌دهد و درنتیجه توقف آن می‌شود. همچنین تحلیل سیاهه ممیزی آسیب‌پذیری‌های دیگری را نشان می‌دهد که هنگام نصب سامانه آشکار نبودند و سخت‌گیری‌های مازادی برای بهبود امنیت سامانه اعمال می‌شود.

این نوع متفاوتی از خدمت برنامه کاربردی و نیز نوع متمایزی از ممیزی است.

دیواره‌های آتش این سوابق ممیزی را ایجاد می‌کنند. سیاهه‌ی مسیریاب ویژه مراقبت بهداشتی نیست.

قابلیت‌های موردنیاز: نیاز به انطباق «از نظر معماری[3]» با آنچه صنعت فناوری اطلاعات برای واپایش خدمت به خطر افتاده انجام می‌دهد، وجود دارد. هم‌چنین این واقعیت که هشدار ارسال شده است، ممیزی می‌شود.

---

1 - Prefetched
2 - Watcher service
3 - Architecturally

الف-۵ نمونه کاربر دارای امتیاز که از امتیاز خود سوءاستفاده می‌کند

فردی از شریک خود درخواست می‌کند که شغلی را به‌عنوان نماینده ثبت سامانه اطلاعاتی/ارائه‌کننده خدمات ثبت داروی جدید بپذیرد و سپس از وی و سایرین به‌عنوان پزشکانی با حقوق تجویز الکترونیک دارو ثبت‌نام می‌کند؛ بنابراین آن‌ها می‌توانند به‌صورت غیرقانونی تجویز دارو داشته باشند.

اغلب در دنیای واقعی تحلیل تصادفی یا مبتنی بر بدگمانی در سیاهه‌های ممیزی، تنها راه آشکار شدن این نوع رویدادها است. سؤال این است که چه طور می‌توانیم به این رویداد به‌موقع پاسخ دهیم؟ آیا ممیزی و نظارت می‌توانند در تشخیص تجویزهای غیرمعمول داروهای تحت بازرسی کمک کنند؟ (مانند افزایش ناگهانی تجویز مورفین) حداقل کمکی که سامانه می‌تواند بکند این است که با کشف کاربر دارای امتیازی که از امتیاز خود سوءاستفاده کرده است، شواهدی از ثبت‌نام‌های غیرمجاز و هم‌چنین فهرستی از همه پزشکان ثبت‌نام‌شده با حساب کاربری دارای امتیاز سوءاستفاده شده، ارائه کند.

قابلیت‌های موردنیاز: رویدادهای ثبت موفق توسط کاربر فهرست شود

قابلیت‌های اختیاری: ارجاع متقابل بین کارساز ممیزی و سایر کارسازها برای تعیین حوزه شکاف

قابلیت‌های بالقوه برای خدمت ID MGMT: تصدیق هویت‌ها در ثبت‌نام ارائه‌کننده در برابر ارائه‌کنندگان اعتبارنامه.

الف-۶ نمونه گمراه‌کننده نتایج آزمایش

شخص تحت مراقبت هم‌اکنون به مدت دو هفته است منتظر نتایج آزمایشگاهی خود است. درحالی‌که پزشک به او گفت که با استفاده از سامانه اطلاعاتی جدید آزمایشگاه نتایج ظرف کمتر از ۴۸ ساعت قابل‌دسترس است. زمانی که وی با مطب پزشک تماس گرفت مطب سابقه سفارش به آزمایشگاه را داشت، اما نتایج را نداشت. پرستار با آزمایشگاه تماس گرفت و پرسید چه اتفاقی برای آزمایش افتاده است. آزمایشگاه سیاهه‌های ممیزی خود را چک کرد و آزمایشگاه دریافت‌کننده را یافت. شماره سفارش و همچنین آزمایشگاه؛ و نتایج در پاسخ ارسال شده است. کاردان آزمایشگاه چک کرد که نتایج به کجا ارسال شده و دریافت که نتایج به مطب پزشک دیگری اشتباهی ارسال شده است. کاردان آزمایشگاه نتایج را به دریافت‌کنندهٔ صحیح دوباره ارسال کرد و فقط برای اینکه مطمئن شود ARR را چک کرد که نتایج به‌درستی مجدد ارسال شده باشد (خروجی رویداد موفق و دریافت‌کنندهٔ صحیح) و با پرستار تماس گرفت و پرسید که آیا وی آنها را دریافت کرده است. پرستار موضوع داده را فراخوانی کرد و مشخص شد نتایج در آن است.

برخی جزئیات اضافی نیاز است به سیاهه‌های ممیزی افزوده شود تا این فرانامه مورد حمایت و پشتیبانی قرار گیرد، به‌طور مثال: ردیابی شماره سفارش، شماره‌های گزارش و غیره. نیاز است تعادلی بین افزودن جزئیات زیاد به سیاهه‌ها و یک تحلیل که می‌تواند سفارش‌ها را با پرس‌وجوها در سیاهه مرتبط کند برقرار شود. یک سؤال برای یافتن جواب این است که: آیا این باید در مدیریت جریان کار انجام شود یا با یک سیاهه ممیزی؟ جهان رادیولوژی این را با مدیریت جریان کار انجام می‌دهد، به‌صورت دوطرفه. (تائید گزارش‌های ارسال‌شده

دریافت می‌شود و همچنین شماره‌های حاوی و غیره). جریان کار گزارش می‌تواند به‌وسیلهٔ یک آزمایشگاه ممیزی مجزا، رسیدگی شود. گزارش‌ها و تائید DB. یک رابط می‌تواند قابلیت مطابقت سیاهه‌های واقعه‌نگاری آزمایشگاه با سایر سیاهه‌های ممیزی را در طول رسیدگی را ایجاد کند. برای مثال: یک خدمت ارتباط سیاهه.

می‌تواند یک گزارش گردش کار و خدمت ممیزی به‌عنوان بخشی از سامانه اطلاعاتی در آزمایشگاه‌ها یا بخش تجویز یا رادیولوژی موجود باشد. یکپارچه‌سازی با تدارکات نیز باید در نظر گرفته شود. (حمل‌ونقل و غیره)

قابلیت موردنیاز: رویدادها، فرستنده و دریافت‌کننده را نشان می‌دهد.

قابلیت بالقوه: نتایج به محل نادرستی فرستاده شد، زیرا خطایی در فهرست ثبت ارائه‌دهنده وجود داشت و این حادثه نیاز به تصحیح/به‌روزرسانی فهرست ثبت ارائه‌دهنده را پوشش نداد. سؤال این است که چگونه این نیاز می‌تواند برای اقدامات اصلاحی به‌طور خودکار راه‌اندازی و برطرف شود؟

این فرانامه متفاوت است که در آن نه یک زمان واقعی نظارت و نه اداره است ولی از سامانه ممیزی برای بررسی گردش کار استفاده می‌شود.

یک کاربر غیر اجرایی در این فرانامه وجود دارد که ممکن است از یک رابط برای مخزن ممیزی استفاده کند که نیاز است کاربرپسند و متفاوت از یک رابط معمولی باشد.

سؤالاتی که در این فرانامه باید بدان پاسخ داده شود بدین شرح است:

- آیا در صورت از دست رفتنِ پیام سامانه قادر به تشخیص آن است؟
- آیا در صورت انجام یک تراکنش سامانه قادر به تشخیص آن است؟ ازآنجاکه تراکنش‌ها رویدادهای ممیزی شده هستند، این اطلاعات باید کسب شوند.
- آیا روشی برای تحلیل وجود یا عدم وجود موفقیت یا شکست پیام‌ها وجود دارد؟
- وقتی یک پیام خطا اتفاق بیفتد (پاسخ با شکست مواجه شود)، آیا این امر با خدمت نظارت مرتبط است؛ برای مثال: اگر سامانه بتواند آن را تشخیص دهد، از دست دادن را گزارش کند.
- برچیدن یک عدم انطباق بین یک اطلاع‌رسانی ارسال و یک اطلاع‌رسانی تحویل، یک کار تطبیق/ تحلیل است که خارج از هدف و دامنه کاربرد یک استاندارد ممیزی است.

شخص امنیتی می‌خواهد مشاهده نماید: اگر شخص درستی پیام آزمایشگاه را در وقت درست دریافت نکند، آیا شخص دیگری در این زمان پیام را خواهد گرفت؟

این بخشی از فرانامه جریان کار/گزارش/کارکرد است. خدمت ممیزی ممکن است بخواهد قابلیت خدمت جریان کار را نشان دهد.

الف-۷ نمونه تراکنش‌های خودسرانه

یک مدیر اجرایی سامانه بیمارستان، متوجه تعداد غیرمعمول از تراکنش‌های شکست‌خورده می‌شود. پس از چک کردن امکانات عیب‌یابی، مدیر اجرایی سامانه می‌تواند تعیین کند که هرچند ساعت یک کاهش شدید پهنای باند رخ می‌دهد، اما دلیل آن مشخص نیست. مدیری اجرایی سیاهه‌ها را چک می‌کند و متوجه می‌شود که نرم‌افزار کاربردی B در حال ارسال دو درخواست از هر یک درخواست آزمایشگاه است و درنتیجه سامانه دچار سربار می‌شود.

این یک نمونه مدیریت اجرایی سامانه و ارزیابی کارکرد است، مشابه فرانامه کارساز در معرض خطر. اطلاعاتی که نیاز است ممیزی شود بسیار متفاوت از موارد امنیتی و حریم خصوصی است.

سامانه ممیزی عمومی می‌تواند در سراسر کشور ثابت بماند و قابلیت‌های مشابهی برای ارسال و ذخیرهٔ سیاهه‌ها استفاده کند. اطلاعاتی که باید ثبت شوند و جایی که آنها باید ثبت شوند به‌وسیلهٔ سیاست‌های پیکربندی محلی تعیین خواهد شد.

در ابتدا، این یک خدمت وب مشارکتی به رابط ARR است که می‌گوید «هر چه غیرعادی است را به من برگردان»، برای مقادیر غیرمعمول مانند «بیش از ۵ باز متولی شکست در ورود به سامانه یا خروجی‌های تراکنش‌های ناموفق».

در دنیای کنونی، این نوع از ممیزی به‌وسیلهٔ ساخت جریان داده‌های خام رسیدگی می‌شود که در دسترس مدیر اجرایی است و با اساسی‌ترین ابزارها تحلیل می‌شود.

سامانه ممکن است نخواهد جزئیات تحلیل را برای جریان ممیزی دریافتی را ارائه دهد اما می‌تواند جریان ممیزی خام را بسازد که از طریق یک رابط برای هرکسی دیگری که بخواهد برای آن تحلیلی بنویسد در دسترس است.

این نمونه می‌تواند گسترش یابد و متغیرهایی مانند نظارت بی‌سیم با استفاده از تجهیزات پزشکی و نظارت از راه دور شخص تحت مراقبت را شامل شود.

الف-۸ نمونه ناپدیدشدن اسناد ممیزی: مخزن ممیزی به‌عنوان هدف

شخصی سعی می‌کند کل مسیرها را پوشش دهد. پایداری در طول زمان برای همهٔ خدمات/سامانه‌ها لازم است به‌منظور اینکه قادر باشد شکاف داده‌ها را اعلان کند؛ زیرا ساده‌ترین چیز برای مهاجم این است که بخشی از ممیزی را در طول حمله یا تراکنش غیرقانونی از کار بیندازد. خاموش کردن انتخابی ممیزی چالش‌برانگیز است، بنابراین اغلب یک شکاف قابل‌توجه وجود دارد. یک ویژگی دوم یک حمله مرتبط با ممیزی خود زمان کارساز است، لذا نیاز به ممیزی دقت و صحت زمان کارساز (آیا بیش از حد معمول بازنشانی[1] شده است؟) و همچنین کارخواه[1]، به‌منظور کشف حوادث بالقوه وجود دارد.

1 - Reset

یادآوری- مسیریاب‌ها یک نقطه مناسب هستند (نزدیک و متصل) که به‌عنوان کارسازهای زمان به‌منظور اطمینان از اینکه همه سامانه‌ها هماهنگ شده است به خدمت گرفته شوند. یک برنامه کاربردی می‌تواند/بهتر است در ترافیک ممیزی به دنبال شکافهای «غیرطبیعی» باشد. ترافیک ممیزی «طبیعی» بهتر است به‌صورت محلی تعریف شود.

ازآنجاکه کارسازهای ممیزی، هدف نخست هستند، چطور می‌توانیم ممیزی کنیم که آیا یک کارساز ممیزی موردحمله واقع شده است یا خیر و برای رفتارهای غیرمعمول باید نظارت انجام دهیم یا خیر و آیا اینها داخل و یا خارج از هدف و دامنه کاربرد خدمات ممیزی است؟

یادآوری ۱- اغلب سامانه‌ها از NTP استفاده می‌کنند که سوابق ممیزی را تولید می‌کند؛ آنها بهتر است در مخزن ممیزی ذخیره شود و نظارت شود.

یادآوری ۲- کارسازهای ممیزی به‌طور طبیعی نیاز دارند از لحاظ فیزیکی محکم شده۲ و حفاظت شوند.

یادآوری ۳- به حفظ رونوشت‌های محلی از سوابق ممیزی توجه شود.

پایداری در طول زمان، قابلیتی است که موردنیاز است و به خدمت ممیزی وابسته است. (نیازاست که استفاده شود و کار کند و نه فقط در دسترس باشد.)

نیازمندی: مخزن ممیزی و خدمات اختصاص داده شده به آن باید محافظت شود، ازجمله واپایش‌های دسترسی و واپایش‌های ممیزی.

الف-۹ نمونه یک نفوذگر که سوابق ممیزی جعلی ایجاد می‌کند:

یک نفوذگر خبره یک لپ‌تاپ وصل کرده که سوابق ممیزی جعلی تولید می‌کند برای اینکه حقیقت را که او سامانه ممیزی را غیرفعال کرده و ماشین تحت حمله است، پنهان کند (برخی از سیاستهای محلی ممکن است برای استفاده از امضاهای دیجیتال به‌منظور تشخیص سوابق ممیزی جعلی انتخاب شود.)

الف-۱۰ نمونه یک نفوذگر که سوابق ممیزی را برداشته و از آنها برای مقاصد سوءاستفاده می‌کند

سوابق ممیزی در تحلیل ترافیک یا تغییرات یا اواسط جریان اطلاعات حیاتی، آسیب‌پذیر باشند.

کاهش خطر: اطلاعات شخصی سلامت را از سوابق ممیزی دور نگه دارید! اگر این غیرممکن است، سوابق ممیزی باید به‌وسیلهٔ ثبت و یا در طول جریان کار/جلسه کدگذاری شود.

---

1 - Client
2 - Hardened

الف-۱۱ نمونه تغییرات غیرعادی پیکربندی (مجاز یا غیرمجاز)

شخصی که نقش مدیر سامانه را ایفا می‌کند، نرم‌افزار سامانه محلی را به‌روز می‌کند (جایگزین: حملهٔ نرم‌افزارهای مخرب/ مهاجم تصادفی یک ثبات http نصب می‌کند و تمام ترافیک را تسخیر می‌کند تا بتواند نقاط آسیب‌پذیری سامانه را تشخیص دهد.)

فرایند ممیزی باید این موارد را ضبط کند: تاریخ، زمان و محل به‌روزرسانی و همچنین «توضیحی از تغییر» که شامل شماره‌های نسخهٔ نرم‌افزار، فایل کنترلی[1] و غیره.

مخزن ممیزی (پیکربندی مخزن ممیزی) باید گاهی اوقات مورد بررسی قرار گیرد به‌منظور اینکه تائید شود که: به‌روزرسانی پیکربندی مجاز و در زمانی که مقرر شده بود صورت گرفته است و تغییرات پیکربندی غیرمنتظره و غیرمجاز مشخص شود.

یک جنبه دیگر از خدمت/سیاهه ممیزی این است که باید همهٔ تغییرات پیکربندی، به‌روزرسانی‌ها و غیره را ثبت کند از قبیل: نصبهای نرم‌افزار، نصبهای سخت‌افزار و تغییرات پیکربندی.

سامانه ممیزی باید اقدام اصلاحی و همچنین تحلیل در زمان واقعی برای تشخیص یک رویداد جانبی در حال پیشروی را حمایت کند.

این مطلوب است اما با تعمیم آن به سخت‌افزار بسیار سخت‌تر می‌شود.

الف-۱۲ نمونه‌ای که یک کاربر سعی می‌کند به یک کلمه‌عبور دست پیدا کند.

کارساز ممیزی گزارش‌های تعدادی ورود ناموفق به سامانه را دریافت کرده و باید سریعاً هشدار لازم در این خصوص را بدهد.

1 - File Checksums

پیوست ب

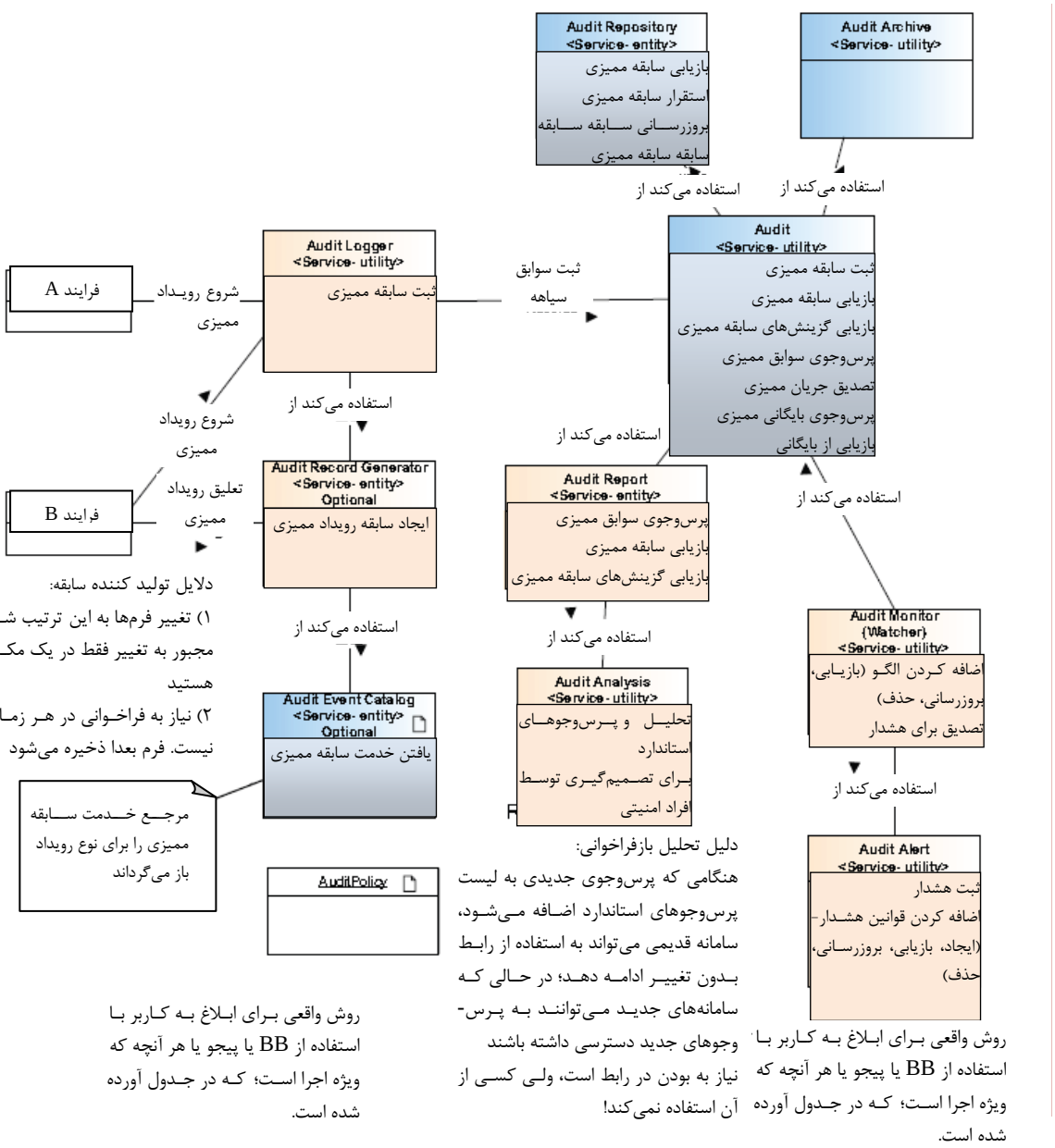
(اطلاعاتی)

خدمات ثبت ممیزی

ب-۱ نمودار خدمات

نمودار گروه ممیزی معماری خدمت‌گرا (SOA)[1] در تصویر ب-۱ نشان داده شده است. این نمودار خدمات ثبت ممیزی ذکرشده در این پیوست را شرح می‌دهد.

1 - Service Oriented Architecture



تصویر ب-۱- نمودار رده ممیزی

ب-۲ خدمت ثبت‌کننده ممیزی

نام قابلیت- ارائه رویداد ممیزی

توضیح- ارائه رویداد ممیزی به‌منظور واپایش

پیش‌شرط-

- سابقه رویداد ممیزی خالی نباشد
- سابقه رویداد ممیزی منطبق با طرح‌واره باشد (سابقه در صورت عدم انطباق رد نخواهد شد).

ورودی‌ها- سابقه رویداد ممیزی (جزئیات TBD)

خروجی- خالی

پس شرط- سابقه تائید می‌شود.

شرایط استثنا-

اگر رویداد ممیزی نتواند ثبت شود، گزارش خطا داده می‌شود. علت این امر آن است که:

- سابقه رویداد ممیزی خالی است؛
- سابقه رویداد ممیزی با طرح‌واره مطابقت ندارد؛
- خدمت به‌طور موقت در دسترس نیست؛
- خدمت غیرقابل‌دسترسی است (مشکل شبکه ارتباطات راه دور).

یادآوری- استثناها می‌توانند در برنامه کاربردی نادیده گرفته شده، اما باید توسط خدمات ممیزی اجرا شوند.

ارتباط با سطوح انطباق

نکات متفرقه- فرضیات:

سامانه باید سازگاری زمانی داشته باشد.

مخزن ذخیره اطلاعات قابلیت گنجایش خروجی برای ارسال خواهد داشت، تا خدمات و پی‌جوها[1] در جایی که سابقه باید بر اساس رویداد فرستاده شود، نظارت شوند.

نیاز به قابلیت ارتباط با طرح‌وارهٔ سابقه رویداد ممیزی مورد انتظار وجود دارد. سامانه‌های خدمت و مشتری هر دو باید دارای سازگاری زمانی باشند تا نتایج معتبر ارائه شود.

(مخزن ذخیره اطلاعات قابلیت گنجایش خروجی را برای ارسال خواهد داشت، تا خدمات و پی‌جوها در جایی که سابقه باید بر اساس رویداد فرستاده شود، نظارت شوند)- این امر در سمت مشتری روی نمی‌دهد، اما نیاز به بررسی‌های آتی وجود خواهد داشت.

سایر محتویات مربوط- در توضیح تفصیلی، می‌خواهیم در مورد انتقال معتبر، ذخیره کردن و نظارت و غیره صحبت نماییم.

1 - Pagers

ب-۳ خدمت تولیدکننده سابقه ممیزی

نام قابلیت- ایجاد سابقه رویداد ممیزی (اختیاری)

توضیح- ایجاد یک سابقه رویداد ممیزی خالی

پیش‌شرط- خالی

- **ورودی**- نوع رویداد ممیزی
- **خروجی‌ها**- سابقه رویداد ممیزی

پس شرط- قالبی از یک سابقه رویداد ممیزی خالی مناسب ایجاد می‌شود. اگر نوع رویداد ممیزی، خالی باشد، یک رویداد ممیزی خالی که شامل کلیه فیلدها از هر نوع رویداد است بازگردانده می‌شود (به‌طور مثال، تمام استانداردهای (DICOM) RFC 3881,ISO 12052:2006، به‌علاوه آنچه در سیاست داخلی به‌عنوان فیلدهای قابل ممیزی موردنیاز تعریف شده است).

شرایط استثنا- نوع رویداد ممیزی مشخص نیست. درصورتی‌که نوع رویداد مشخص نباشد، قابلیت هشدار و لیست کاملی از انواع رویدادهای شناخته شده به اضافه طرح‌وارهٔ فیلدهای احتمالی را برمی‌گرداند.

ارتباط با سطوح انطباق- TBD

نکات متفرقه

هدف از این قابلیت، ایجاد توانایی در تغییر طرح‌واره در یک محل است و به همه برنامه‌های کاربردی این امکان را می‌دهد تا متوجه تغییر طرح‌واره شده و سپس طرح‌واره‌ای را که مورد استفاده قرار می‌دهند را بدون هیچ تغییر کدی به‌روزرسانی کنند.

به‌علاوه می‌تواند به برنامه کاربردی اطلاع دهد که برای ایجاد رویداد ممیزی چه اطلاعاتی موردنیاز است. همچنین این قابلیت به شما انعطاف‌پذیری می‌دهد تا بیش از یک مخزن داشته باشید، یا داده‌ها را هم به‌صورت محلی و هم خارج از سامانه و در مکان دور ثبت و ذخیره نمایید، بدون اینکه مشتری چیزی در مورد آن بداند.

تولیدکننده سابقه ممیزی می‌تواند از فهرست رویداد ممیزی، برای تعیین طرح‌وارهٔ مناسب نوع رویداد مورد درخواست استفاده کند و طرح‌وارهٔ مناسبی را برای نوع رویداد درخواست شده مشخص نماید. این امر با استثنایی که برای طرح‌وارهٔ نامناسب در ثبت‌کننده ممیزی وجود دارد، به مشتری این امکان را می‌دهد که تشخیص دهد چه زمانی کپی محلی طرح‌وارهٔ ذخیره‌شده، تاریخ گذشته و منسوخ شده است. همچنین اجازه اصلاح و بازبینی را بدون هرگونه تغییر کد برای توزیع به مشتریان می‌دهد.

سایر محتویات مربوط

این، خدمت اختیاری است. مجریان مجرب پاسخ را در سمت مشتری ذخیره می‌کنند تا در مورد شِماهایی که تغییر نیافته‌اند صرفه‌جویی زمانی شود.

ب-۴ خدمت فهرست رویداد ممیزی

نام قابلیت- یافتن خدمت رویداد ممیزی

توضیح- طرح‌وارهٔ رویداد ممیزی را به نوع مورد درخواست ارجاع می‌دهد. این خدمت به‌طور مستقیم برای مشتری آشکار نیست؛ اما برای استفاده در اختیار خدمات ثبت‌کننده ممیزی و تولیدکننده سابقه رویداد ثبت قرار داده شده است.

پیش‌شرط- خالی

- **ورودی‌ها**- نوع رویداد ممیزی
- **خروجی‌ها**- طرح‌وارهٔ رویداد ممیزی

ثابت‌ها

پس شرط‌ها

شرایط استثنا- نوع رویداد ممیزی نوع مشخصی نیست.

ارتباط با سطوح انطباق

نکات متفرقه

این گروه، موقعیت مرکزی طرح‌وارهٔ رویداد ممیزی را مشخص می‌کند و باید به‌عنوان منبع رونوشت‌های محلی شِما برای سامانه مشتری مورد استفاده قرار گیرد. شِماها به‌واسطه تولیدکننده سابقه ممیزی می‌توانند به‌طور خودکار به مشتریان انتشار یابند.

سایر محتویات مربوط

این خدمت صرفاً یک خدمت زمینه‌ای است که به‌طور غیرمستقیم از طریق خدمات قبلی در اختیار مشتری قرار می‌گیرد.

ب-۵ خدمت نظارت ممیزی

یادآوری- هشدار به‌عنوان پیامی تعریف می‌شود که زمانی که خدمت نظارت متوجه انطباق مجموعه‌ای از حوادث با یک الگو می‌شود، ارسال می‌گردد.

نام هشدار به‌عنوان الگویی از رویدادهایی تعریف می‌شود که دارای اسم منحصربه‌فردی هستند؛ به‌طور مثال «جستجوی شناسه فاعل داده». در زندگی واقعی، درصورتی‌که نگرانی در مورد شخصی که داده فاعلی را جاسوسی می‌کند وجود داشته باشد، هرگونه دسترسی به اطلاعات فاعل داده باید هشداری ایجاد کند.

نام قابلیت- تصدیق هشدار

توضیح- توسط خدمات هشدار ممیزی فراخوانی می‌شود تا به خدمت نظارت امکان آگاهی در این مورد را بدهد که خدمت هشدار ممیزی خواهان اطلاع‌رسانی در زمان وجود یک هشدار امنیتی است.

پیش‌شرط- نام هشدار معتبر است، به‌طور مثال نام هشدار الگویی دارد که به سامانه افزوده شده است.

ورودی‌ها

- نام هشدار (یادآوری- برخی اسامی هشدار ممکن است از قبل تعریف شده باشند، در غیر این صورت تنها الگوهای اضافه شده هستند).
- تصدیق‌کننده منبع (یادآوری قالب- در SOAP، آدرس نقطه پایانی خدمت وب است و در جاوا آدرس رابط کاربری است. مرجع باید منحصربه‌فرد باشد تا از بروز تصادم جلوگیری شود).

خروجی‌ها- خالی

ثابت‌ها

پس‌شرط‌ها

- خدمت هشدار ممیزی که فراخوانی می‌شود اکنون به نظارت ممیزی مشهور است.
- استثنا نام هشدار غیرمعتبر را شرط می‌کند.

نکات متفرقه

فرضیه- هر شخص در مورد یک زبان الگو به توافق رسیده است.

به‌منظور «تصدیق **و** به‌دست‌آوردن تاریخچه رویدادهای ساعت آخر» رابط می‌تواند هر دو قابلیت را **به اضافه** سوابق ممیزی پرس‌وجو از خدمت گزارش ممیزی فراخوانی کند.

یادآوری- نیاز به تعیین چگونگی کسب و استفاده از پارامتری وجود دارد که به تصدیق‌کننده امکان تعیین زمان انقضای تصدیق را بدهد.

انقضای تصدیق- هیچ تاریخ برای خدمت نظارت تعیین نشده است. اگر مشتری خواهان انقضای تصدیق باشد، اجرای خدمت هشدار/ ابلاغیه، می‌تواند برنامه زمانی تصدیق را تعیین کند.

نام قابلیت- عدم تصدیق هشدارها

توضیح- توسط خدمت هشدار ممیزی فراخوانی می‌شود تا به خدمت نظارت، امکان آگاهی از اینکه خدمت هشدار ممیزی دیگر تمایلی به اطلاع از حوادث ممیزی ندارد را بدهد.

یادآوری- توجه داشته باشید که تصدیق خدمت نظارت مانند تصدیق خدمت ابلاغیه نیست. تصدیق خدمت ابلاغیه توسط افرادی در زمان‌های مختلف انجام می‌شود. درحالی‌که تصدیق خدمت نظارت توسط خدمتی مانند خدمت ابلاغیه انجام می‌شود. درواقع خدمت نظارت، خدمت ساده‌تری است که برای انطباق الگو طراحی شده است و هشدار و ابلاغیه‌ی سطح بالایی ارائه نمی‌دهد.

پیش‌شرط

ورودی‌ها

- نام هشدار
- مرجع تصدیق

خروجی‌ها- خالی

پس شرط‌ها- تصدیق دیگر ثبت نمی‌شود.

شرایط استثنا

ارتباط با سطوح انطباق

نکات متفرقه

سایر محتویات مربوط- ارسال یک رویداد ممیزی!

نام قابلیت- افزودن الگو

توضیح- به خدمت هشدار ممیزی امکان تعیین نوع جدیدی از الگوی رویداد را برای جستجو می‌دهد. برای این منظور از مشخصه چگونگی تعیین وقوع موقعیت قابل هشدار استفاده می‌شود.

پیش‌شرط-

- نام هشدار خالی نیست و منحصربه‌فرد است.
- الگوی رویداد خالی نیست و به‌طور مناسب مشخص شده است.

ورودی‌ها- نام هشدار، الگوی رویداد

خروجی‌ها- خالی

پس شرط‌ها- الگوی جدید به آن‌هایی که نظارت هشدار از آن مطلع است اضافه می‌شود که با نامِ نام هشدار (alertName) در ارتباط است.

شرایط استثنا-

- نام هشدار از قبل وجود دارد
- نام هشدار خالی است
- الگوی رویداد معتبر نیست

ارتباط با سطوح انطباق

نکات متفرقه

فرضیه- هر شخص بر سر یک زبان الگو به توافق رسیده است.

فرضیه- الگوها به نوعی با ایجادکننده در ارتباط هستند.

سیاست دسترسی به یک نمونه ویژه می‌تواند این باشد: «این کاربر/URL/ و غیره می‌تواند تغییر دهد.»

سایر محتویات مربوط- ارسال رویداد ممیزی

نام قابلیت- الگوی بازیابی

توضیح- این امکان را به خدمت هشدار ممیزی می‌دهد تا الگویی را بازیابی کند. اگر نام هشدار معتبر نبوده و یا خالی باشد، لیستی از کلیه‌ی الگوها را باز می‌گرداند.

پیش‌شرط

ورودی‌ها- نام هشدار

خروجی‌ها- جزئیات نمونه یا لیستی از تمام الگوهای ثبت شده و یا قابل‌دسترس

پس شرط‌ها- الگو یا سیاهه‌ای از الگوها

شرایط استثنا- وجود ندارد

نکات متفرقه

این رویداد، خود یک رویداد قابل ممیزی است. همچنین تا حدودی سیاست داخلی است که تعیین می‌نماید آیا خدمتی است که رویداد ممیزی را ارسال نماید یا برنامه کاربردی است که از آن استفاده کند. به‌بیان‌دیگر باید مجریان در مورد آن تصمیم‌گیری کنند.

سایر محتویات مربوط- اختیاری- ارسال رویداد ممیزی

نام قابلیت- حذف الگو

توضیح- الگویی را که دیگر کاربردی نیست حذف می‌کند. درصورتی‌که هنوز شنوندگان تصدیق شده‌ای برای الگو وجود داشته باشند و پارامتر حذف اجباری موجود و درست باشد، حذف، حذفِ اجباری است. چنانچه پارامتر موجود و درست نباشد و شنوندگان قابل تصدیق نیز وجود داشته باشند، پارامتر حذف با شکست مواجه می‌شود و استثنایی به درخواست‌کننده ارسال می‌گردد.

پیش‌شرط- نام هشدار خالی نیست

ورودی

- نام هشدار
- پارامتر حذف اجباری

خروجی‌ها- خالی

پس شرط‌ها

- الگو و کلیه تصدیق‌کنندگان آن الگو حذف می‌شوند.
- به عبارتی خروجی خالی است.

شرایط استثنا- اگر تصدیق‌کنندگان هشدار و حذف اجباری موجود و درست نباشند، استثنایی در برابر درخواست حذف ارسال می‌شود.

ارتباط با سطوح انطباق

نکات متفرقه- حذف شنوندگان باید به اطلاع صادرکننده پیام و یا شنوندگان برسد.

«افزایش یک رویداد» را فراموش نکنید؛ چراکه هنوز تصدیق‌کنندگانی وجود دارند. سایر واپایش‌ها و شنیدن تصدیق‌کنندگان می‌تواند برای اجرا کنار گذاشته شوند.

در صورت شکست حذف، الگوی حذف باید لیستی از تصدیق‌کنندگان باقی‌مانده را ارسال نماید.

سایر محتویات مربوط- ارسال رویداد ممیزی

ب-۶ خدمت هشدار یا ابلاغیه

نام قابلیت- اعلان ابلاغیه

توضیح- پیام هشدار را برای واپایش اعلان می‌کند.

پیش‌شرط

ورودی‌ها- پیام ابلاغیه

خروجی‌ها- خالی

پس شرط‌ها- پیام هشدار طبق قوانین قابل اجرا ارسال می‌شود.

شرایط استثنا

- پیام هشدار خالی است.
- خطای پردازش پیام هشدار

ارتباط با سطوح انطباق

نکات متفرقه

روش واقعی برای ابلاغ به کاربر (مانند پی‌جو یا سایر رسانه‌ها) روش خاصی است که ویژه اجرا است.

سایر محتویات مربوط- ارسال رویداد ممیزی پس از اعلان هشدار

نام- تدوین مجموعه قانون ابلاغیه

توضیح- ایجاد و حفظ قوانینی که چگونگی واپایش یک پیام هشدار را تعیین می‌کنند، یا به عبارتی موقعیت ارسال آن را مشخص می‌سازد.

پیش‌شرط- مجموعه قوانین هشدار خالی نیست.

فرمت مجموعه قوانین هشدار باید مشخص شده و توسط خدمت قابل پردازش باشد.

ورودی‌ها- مجموعه قوانین ابلاغیه

خروجی‌ها- خالی

پس شرط- مجموعه قوانین ابلاغیه جدید هماهنگ است.

شرایط استثنا

- قانون هشدار خالی است
- قانون نامشخص

ارتباط با سطوح انطباق

نام قابلیت- قوانین هشدار بازیابی

توضیح- یک کپی از قوانین هشدار اخیر اجباری بر این خدمت را بازیابی می‌کند.

پیش‌شرط- چیزی وجود ندارد

ورودی‌ها- چیزی وجود ندارد

خروجی‌ها- قوانین هشدار

ثابت‌ها- قوانین هشدار تغییر نمی‌یابند.

پس شرط‌ها- قوانین هشدار خروجی شامل مجموعه‌ی کاملی از قوانین هشدار اجباری است.

شرایط استثنا- چیزی وجود ندارد

ارتباط با سطوح انطباق

نکات متفرقه

سایر محتویات مربوط

ب-۷ خدمت گزارش ممیزی

نام- خدمت ممیزی پرس‌وجو

توضیح- از خدمت ممیزی برای انطباق سوابق با الگو یا پارامترهای پرس‌وجوی درخواست شده در صافی[1] پرس‌وجو می‌کند

پیش‌شرط- صافی پرس‌وجو خالی نیست. اگر تمام سوابق درخواست شوند، الگویی (هم ارزی با زبان پرس-وجو) باید استفاده شود.

زبان صافی پرس‌وجو باید مورد توافق باشد

ورودی‌ها- صافی پرس‌وجو

خروجی‌ها- لیستی از شناسه‌های منحصربه‌فرد سوابق درخواست شده

پس شرط‌ها- شناسه سابقه با صافی پرس‌وجوی برگردانده شده مطابقت دارد.

شرایط استثنا

- صافی جستجو خالی است
- صافی جستجو نمی‌تواند تجزیه شود

ارتباط با سطوح انطباق

نکات متفرقه

سایر محتویات مربوط

نام- سابقه ممیزی بازیابی

---

1 -Filter

توضیح- سابق ممیزی خاصی را بازیابی می‌کند

پیش‌شرط- شناسه سابقه خالی نیست

ورودی‌ها- شناسه سابقه

خروجی‌ها- سابقه درخواست شده، در صورت وجود. در غیر این صورت خالی است.

پس شرط‌ها- سابقه متناظر با شناسه سابقه برگردانده می‌شود

شرایط استثنا- شناسه سابقه خالی است

نام- گزینش سابقه ممیزی بازیابی

توضیح- گزینشی را که توصیف‌های فیلد از سابقه با شناسه سابقه انطباق دارد، بازیابی می‌کند.

پیش‌شرط- شناسه سابقه خالی نیست

توصیف‌های فیلد معتبر است.

ورودی‌ها

- شناسه سابقه
- توصیف‌های فیلد

خروجی‌ها- در صورت وجود شناسه، گزینش سابقه ممیزی منطبق با فیلدهای درخواست شده از سابقه‌ای است که شناسه آن مطابقت دارد. در غیر این صورت، خالی است.

پس شرط‌ها- گزینش درخواست شده برگردانده می‌شود

شرایط استثنا

- شناسه سابقه خالی است
- توصیف‌های فیلد معتبر نیست

ارتباط با سطوح انطباق

ب-۸ خدمت تحلیل ممیزی

نام قابلیت- تحلیل

توضیح- انجام تحلیل درخواست شده

پیش‌شرط- تحلیل درخواست، یک الگوریتم معتبر است

ورودی‌ها- الگوریتم تحلیل

خروجی‌ها- گزارش تحلیل

پس شرط‌ها- تحلیل الگوریتم انجام شده است و نتایج برگردانده شده است

شرایط استثنا- الگوریتم تحلیل نامعتبر است

ارتباط با سطوح انطباق

کتاب‌نامه

[1] ISO 12052:2006, Health informatics — Digital imaging and communication in medicine (DICOM) including workflow and data management

[2] ISO/TS 14265:2011, Health Informatics - Classification of purposes for processing personal health information

[3] ISO 15489-1:2001, Information and documentation — Records management — Part 1: General

[4] ISO/TS 21298:2008, Health informatics — Functional and structural roles

[5] ISO/TS 21547:2010, Health informatics — Security requirements for archiving of electronic health records — Principles

[6] ISO/TS 22600 (all parts), Health informatics — Privilege management and access control

[7] ISO/IEC 8824-1, Information technology — Abstract Syntax Notation One (ASN.1): Specification of basic notation — Part 1

[8] ISO/IEC 8824-2, Information technology — Abstract Syntax Notation One (ASN.1): Information object specification — Part 2

[9] ISO/IEC 15408-2:2008, Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components

[10] ASTM E2147-01, Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems

[11] DICOM. Supplement 95: Audit Trail Messages, Final Text 27 August 2010, now incorporated in DICOM Part 15: http://medical.nema.org/standard.html

[12] IHE IT Infrasructure Technical Framework, Volume 1: Integration Profiles and Volume 2: Transactions

[13] IETF RFC 3881:2004, Security Audit & Access Accountability Message — XML Data Definitions for Healthcare Applications

[14] ISO/IEC 2382-8:1998, Information technology — Vocabulary — Part 8: Security

[15] ISO 7498-2, Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture

[16] ISO/IEC 27000:2012, Information technology — Security techniques — Information security management systems — Overview and vocabulary

[17] ASTM E1769:1995, Standard Guide for Properties of Electronic Health Records and Record Systems

[18] IEC 60050-713:1998, International Electrotechnical Vocabulary — Part 713: Radiocommunications: transmitters, receivers, networks and operation

[19] IETF RFC 4810, Long-Term Archive Service Requirements

[20] IETF RFC 4998, Evidence Record Syntax (ERS)