INSO
16289-1
1st. Edition
May.2013

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

استاندارد ملی ایران
۱-۱۶۲۸۹
چاپ اول
اردیبهشت ۱۳۹۲

اطلاع رسانی سلامت – مدیریت امنیت اطلاعات برای نگهداری از راه دور وسایل پزشکی و سیستم های اطلاعات پزشکی - قسمت ۱: الزامات و تحلیل ریسک

Health informatics – Information security management for remote maintenance of medical devices and medical information systems – Part 1 : Requirement and risk analysis

ICS: 35.240.80

بنام خدا

آشنایی با سازمان ملی استاندارد ایران

سازمان ملی استاندارد ایران به موجب بند یک مادهٔ۳ قانون اصلاح قوانین و مقررات سازمان ملی استاندارد ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.
تدوین استاندارد در حوزه های مختلف در کمیسیون های فنی مرکب از کارشناسان سازمان صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می شود وکوششی 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 وارد کنندگان، مراکز علمی و تخصصی، نهادها، سازمان های دولتی و غیر دولتی حاصل می شود .پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی(رسمی) ایران چاپ و منتشر می شود.
پیش نویس استانداردهایی که مؤسسات و سازمان های علاقه مند و ذیصلاح نیز با رعایت ضوابط تعیین شده تهیه می کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می شود .بدین ترتیب، استانداردهایی ملی تلقی می شود که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می‌دهد به تصویب رسیده باشد.
سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)[1] کمیسیون بین المللی الکتروتکنیک (IEC)[2] و سازمان بین المللی اندازه شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی های خاص کشور، از آخرین پیشرفتهای علمی، فنی و صنعتی جهان و استانداردهای بین المللی بهره‌گیری می‌شود.

سازمان ملی استاندارد ایران می تواند با رعایت موازین پیش بینی شده در قانون، برای حمایت از مصرف کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشو ر و / یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سا زمانها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش ، سازمان استاندارد این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آنها نظارت می کند .ترویج دستگاه بین المللی یکاها، کالیبراسیون (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 Electro technical Commission
3- International Organization for Legal Metrology (Organization International de Metrology Legal)
4 - Contact point
5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

« اطلاع رسانی سلامت – مدیریت امنیت اطلاعات برای نگهداری از راه دور وسایل پزشکی و سیستم های اطلاعات پزشکی - قسمت ۱: الزامات و تحلیل ریسک »

	سمت و/ یا نمایندگی
رئیس:	
صیادی ، سعید (فوق لیسانس الکترونیک)	شرکت بهساز طب
دبیر:	
رزق دوست ، غلامحسین (لیسانس بیولوژی ، فوق لیسانس مدیریت اجرایی)	پژوهشگاه استاندارد
اعضاء: (اسامی به ترتیب حروف الفبا)	
احمد زاده ، بهاره (لیسانس پرستاری)	بیمارستان فوق تخصصی البرز کرج
داوودی ، ابوالفضل (فوق لیسانس میکروبیولوژی)	انجمن صنفی تجهیزات پزشکی
رجبعلی ، ساناز (فوق لیسانس مهندسی پزشکی)	شرکت مدیریت تجهیزات پزشکی
صانعی ، کامران (لیسانس مدیریت)	شرکت مدیریت تجهیزات پزشکی
فائقی ، فرانک (فوق لیسانس فیزیک پزشکی)	پژوهشگاه استاندارد
فرجی ، رحیم (لیسانس شیمی)	پژوهشگاه استاندارد
کلیشادی ، احمد رضا (لیسانس مهندسی برق و الکترونیک)	مرکز تحقیقات انفورماتیک

گرجی ، زهرا
(لیسانس شیمی کاربردی)
شرکت سها

مخنفی ، محمد تقی
(لیسانس مهندسی شیمی)
شرکت ساخت وسایل پزشکی ایران
(سوپا)

فهرست مندرجات

عنوان **صفحه**

پیش گفتار

استاندارد" اطلاع رسانی سلامت – مدیریت امنیت اطلاعات برای نگهداری از راه دور وسایل پزشکی و سیستم های اطلاعات پزشکی - قسمت ۱: الزامات و تحلیل ریسک "که پیش نویس آن درکمیسیون های مربوط توسط سازمان ملی استاندارد ایران تهیه و تدوین شده و در صد و سی و پنجمین اجلاس کمیتهٔ ملی استاندارد خدمات مورخ ۹۱/۷/۸ مورد تصویب قرار گرفته است ، اینک به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات سازمان ملی استاندارد ایران، مصوب بهمن ماه ۱۳۷۱ ، به عنوان استاندارد ملی ایران منتشر می‌شود .

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت های ملی و جهانی در زمینهٔ صنایع، علـوم و خـدمات، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح و تکمیل ایـن استانداردها ارائه شود، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفـت . بنـابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی استفاده کرد.

منبع و ماخذی که برای تهیهٔ این استاندارد مورد استفاده قرار گرفته به شرح زیر است:

ISO / TR 11633-1 : 2009 : Health informatics – Information security management for remote maintenance of medical devices and medical information systems – Part 1 : Requirement and risk analysis

مقدمه

پیشرفت و گسترش فن آوری در عرصه ارتباطات و اطلاعات و چیدمان مناسب زیر ساخت ها ی استقرار یافته بر پایه آن ها، تغییرات وسیعی در جامعه مدرن کنونی ایجاد کرده است. در عرصه حفظ سلامت، سیستم های اطلاعات که قبلا در هریک از مراکز حفظ سلامت محصور شده بودند، هم اکنون توسط شبکه ها به هم مرتبط شده و تا آن جا پیش رفته اند که قادرند استفاده دوسویه از اطلاعات سلامت ذخیره شده در هر سیستم اطلاعات را تسهیل نمایند.

اینگونه شبکه های اطلاعات و ارتباط نه تنها در میان مراکز حفظ سلامت، بلکه در میان مراکز حفظ سلامت و فروشندگان وسایل پزشکی یا سیستم های اطلاعات حفظ سلامت برقرار شده اند. با بکار گیری خدمات نگهداری از راه دور (RMS[1])، کاهش زمان از کار افتادن (خواب) تجهیزات و دستیابی به هزینه های پایین تر امکان پذیر می گردند.

بر اساس اطلاعات ارائه شده در این استاندارد، مراکز حفظ سلامت و تامین کنندگان خدمات سرویس ونگهداری از راه دور قادر به انجام فعالیت های زیر می باشند:

- شفاف سازی ریسک های ناشی از خدمات نگهداری از راه دور، به هنگامی که شرایط محیطی محل فروش مورد درخواست مرکز خدمات سرویس و نگهداری از راه دور (RSC) و مراکز نگهداری حفظ سلامت هدف گذاری شده مرکز حفظ سلامت (HCF) از پیوست الف انتخاب شوند.
- اخذ ضروریات لازم برای انتخاب و استقرار کنترل های فنی و غیر فنی برای اعمال در آن مراکز برای کنترل ریسک های تشریح شده در این استاندارد.
- در خواست سوابق اقدامات پیشگیرانه مشخص از شرکای تجاری که می توانند ریسک های ایمنی مرتبط را تعیین کنند.
- شفاف سازی مرز مسئولیت بین مراکز حفظ سلامت و تامین کننده خدمات سرویس ونگهداری از راه دور؛
- طرح ریزی یک برنامه برای شفاف سازی ریسک های موجود یا انتقال یافته با انتخاب کنترل های مناسب.

با استقرار فرایند ارزیابی ریسک و بکار گیری کنترل ها با ارجاع به این استاندارد، مراکز حفظ سلامت و تامین کنندگان خدمات نگهداری از راه دور قادر به کسب فواید زیر خواهند بود :

- ارزیابی ریسک فقط برای آن محیط های سازمانی ضروری است که این استاندارد در مورد آن ها کاربرد ندارد، بنابر این تلاش برای ارزیابی ریسک به میزان قابل توجهی کاهش می یابد.
- به نمایش گذاشتن اعتبار اقدامات پیشگیرانه مربوط به ایمنی نگهداری از راه دور برای شخص ثالث با سهولت بیشتر انجام می شود.

1-Remote maintenance services

- چنانچه خدمات نگهداری از راه دور برای دو یا چند مرکز تامین شود، تامین کننده می تواند اقدامات پیشگیرانه را با کارآئی و اثر بخشی بیشتر برای آن ها اعمال نماید.

اطلاع رسانی سلامت – مدیریت امنیت اطلاعات برای نگهداری از راه دور وسایل پزشکی و سیستم های اطلاعات پزشکی - قسمت ۱: الزامات و تحلیل ریسک

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد تعیین الزامات در مورد سیستم های اطلاعات در مراکز حفظ سلامت، بر خدمات سرویس و نگهداری از راه دوری(RMS)تمرکز دارد که توسط فروشندگان وسایل پزشکی یا سیستم های اطلاعات سلامت (تامین کنندگان RMS) تامین می شود، و همچنین یک مثال از روش اجرای تحلیل ریسک برای محفوظ نگهداشتن اطلاعات هر دو طرف ذینفع (پیش از هر چیز، خود سیستم اطلاعات و داده های سلامت اشخاص) در یک قالب ایمن و کار آمد (به عنوان مثال اقتصادی) را نشان می دهد.

این استاندارد شامل موارد زیر است :

- فهرستی از موضوعات (کاتالوگ) مورد استفاده برا ی خدمات سرویس ونگهداری از راه دور؛
- فهرستی از تامین کنندگان ذخائر اطلاعات در مراکز حفظ سلامت (HCF) و خدمات نگهداری از راه دور؛
- یک مثال از تحلیل ریسک بر اساس موارد استفاده.

۲ اصطلاحات و تعاریف

در این استاندارد اصطلاحات و تعاریف زیر بکار می روند :

۲-۱

قابل اتکا بودن

خصوصیتی که اطمینان می دهد که فعالیت های یک نهاد تنها بصورت منحصر به فرد به آن نهاد قابل رد یابی است

(تعریف ۲-۱ از استاندارد ISO/IEC 13333-1 : 2004)

۲-۲

ذخائر (اندوخته)

هر چیز با ارزش برای سازمان

یادآوری ۱ – اقتباس شده از استاندارد ISO / IEC 13335-1

یادآوری ۲- در مقوله های امنیت اطلاعات سلامت، ذخائر اطلاعات شامل موارد زیر است :

الف) اطلاعات سلامت

ب) خدمات فن آوری اطلاعات (IT)

پ) سخت افزار

ت) نرم افزار

ث) تسهیلات ارتباطاتی

ج) محیط های انتقال اطلاعات[1]

چ) تسهیلات فن آوری اطلاعات

ح) آن وسایل پزشکی که داده ها را ثبت یا گزارش می کنند

۳-۲

تضمین

نتیجه یک دسته از فرآیند های مطابقت است که از طریق آن یک سازمان به قابل اطمینان بودن وضعیت مدیریت ایمنی اطلاعات خود دست می یابد

۴-۲

قابلیت دسترسی

در دسترس قرار داشتن و قابل استفاده بودن بر اساس در خواست یک نهاد ذیصلاح (تعریف ۲-۴ از استاندارد ISO /IEC 13335-1:2004)

۵-۲

ارزیابی مطابقت

فرآیند هایی که یک سازمان توسط آن ها تایید می کند که کنترل های پیاده شده برای امنیت اطلاعات بصورت کارآمد و عملیاتی کار می کنند

یادآوری- به صورت مشخص، کنترل های پیاده شده در سایت برای سازگاری با الزامات قانونی مرتبط برای حفاظت از داده های شخصی، (مانند دایرکتیو اتحادیه اروپا در خصوص حفاظت از اطلاعات فردی)، مطابقت قانونی نامیده می شود.

۶-۲

راز داری

خصوصیت محفوظ بودن اطلاعات و عدم فاش شدن آن ها برای اشخاص غیر مجاز، نهاد ها یا فرآیند ها را گویند

1- Media

(تعریف ۲-۶ استاندارد ISO/IEC 13335-1:2004)

۷-۲

یکپارچگی داده

خصوصیت عدم تغییر یا عدم تخریب داده به روشی غیر مجاز را گویند

(تعریف ۳-۱-۱ استاندارد ISO / IEC 9797-1:1999)

۸ -۲

نظارت بر اطلاعات

فرآیندی است که توسط آن یک سازمان اطمینان حاصل می نماید که ریسک های مرتبط با اطلاعات سازمان، و از این طریق توانایی های عملیاتی و یکپارچگی سازمان بصورت کارآمد تعیین و مدیریت شده است

۹-۲

امنیت اطلاعات

حفظ راز داری، یکپارچگی و قابل دسترس بودن اطلاعات را گویند

۱۰-۲

ریسک

ترکیب احتمال وقوع یک حادثه و پی آمد های ناشی از آن را گویند

(تعریف ۳-۱-۱ راهنمای ISO/IEC 73:2002)

۱۱-۲

ارزیابی ریسک

فرآیند کلی سنجش و تحلیل ریسک را گویند

(تعریف ۳-۳-۱ از راهنمای ISO / IEC 73: 2002)

۱۲-۲

مدیریت ریسک

فعالیت های هماهنگ برای هدایت و کنترل یک سازمان در ارتباط با ریسک

یادآوری- مدیریت ریسک بصورت نوعی شامل ارزیابی ریسک ، تعدیل ریسک ، پذیرش ریسک و تبادل ریسک می باشد
(تعریف ۳-۱-۷ راهنمای ISO /IEC 73:2002)

۱۳-۲

تعدیل ریسک

فرآیند انتخاب و استقرار اقداماتی برای تعدیل (بصورت نوعی کاهش) ریسک را گویند

یادآوری- برگرفته از راهنمای ISO / IEC guide 73 :2002

۱۴-۲

یکپارچگی سیستم

خصوصیتی که یک سیستم، کارکرد مورد نظر را با یک روش بدون مشکل و به دور از دست کاری های غیر مجاز تصادفی یا عمدی به انجام می رساند

۱۵-۲

تهدید

علت بالقوه یک حادثه نا خواسته که می تواند سبب صدمه به یک سیستم یا سازمان شود

یادآوری- مطابق با استاندارد ISO / IEC 13335-1

۱۶-۲

آسیب پذیری

نقطه ضعف در یک یا گروهی از ذخائر اطلاعات که می تواند توسط یک تهدید در مخاطره قرار گیرد

یادآوری- مطابق با استاندارد ISO /IEC 13335-1

۳ واژه های اختصاری

- HCF[1] : مرکز حفظ سلامت
- ISP[2]: برنامه سرقت اطلاعات
- PHI[3] : اطلاعات سلامت شخصی
- RMS[4] :خدمات سرویس و نگهداری از راه دور

1-Health care facility
2-Information stealing program
3-Pesonal health information
4-Remote maintenance services

- RSC[1] : مرکز خدمات نگهداری از راه دور
- RSS [2]: امنیت خدمات سرویس ونگهداری از راه دور
- VPN[3]: شبکه مجازی خصوصی

۴- یک طرح کلی از امنیت خدمات نگهداری از راه دور

۴-۱ محتوای امنیت خدمات نگهداری از راه دور

۴-۱-۱ کلیات

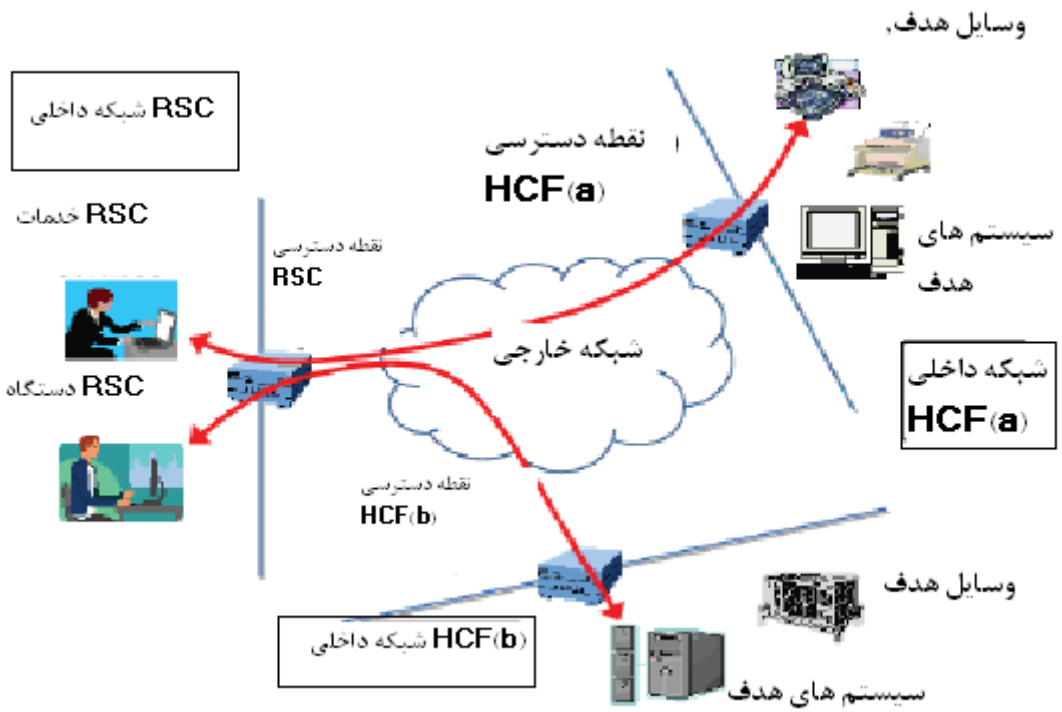
خدمات نگهداری از راه دور دارای سه هدف اصلی است::

- پاسخ دهی در زمانی که تجهیزات پزشکی به درستی کار نمی کند
- نگهداری معمول [4]
- به روز کردن نرم افزار

در این استاندارد یک سیستم فرضی شامل وسایل هدف و یک شبکه داخلی در سایت یک مرکز حفظ سلامت (HCF)، یک شبکه ارتباطی بیرونی که HCF را به مرکز خدمات نگهداری از راه دور(RSC) مرتبط می کند، و یک شبکه داخلی و تجهیزات یا خدمات در درون یک RSC در نظر گرفته شده است. به شکل ۱ مراجعه شود.

این استاندارد شیوه های مختلف سیستم تامین خدمات نگهداری از راه دور (RMS) که توسط تامین کنندگان آن مورد استفاده قرار می گیرند و همچنین موقعیت اقدامات امنیتی جاری را معرفی می نماید.

1-Remote maintenance service center
2-Remote maintenance service security
3- Virtual private network
4- Routine



شکل ۱ - یک سیستم فرضی خدمات نگهداری از راه دور

۴-۱-۲ قالب های مختلف خدمات نگهداری از راه دور و اقدامات فنی مرتبط با امنیت

۴-۱-۲-۱ خدمات نگهداری از راه دور با استفاده از یک شبکه تلفن عمومی سوئیچ شده

HCF برای کارکرد سرور مربوط از طریق شماره گیری[1] ، یک ماشین را آماده و تنظیم می کند. این ماشین از طریق مودم و سایر ملزومات به یک شبکه تلفن عمومی سوئیچ شده مرتبط شده و برای دسترسی از طریق تجهیزات کنترل از راه دورRSC منتظرمی ماند. وسایل ارتباط از راه دور که کلیه عملیات نظیر روتر های شماره گیری ها را ارائه می نمایند در عرصه وسیعی موجود می باشند.

برای استفاده از شبکه تلفن سوئیچ شده، خطوط ارتباط راه دور واجد خصوصیت های زیر می باشند:

- یک مسیر ارتباطی یک به یک بین HCF و RSC می تواند بصورت ایمن برقرارشود.
- بدلیل دیجیتالی بودن کامل شبکه تلفن سوئیچ شده، سوء استفاده از آن دشواراست.

با استفاده از این خصوصیات و اقدامات فنی زیر امنیت برقرار می گردد:

1-Dial up

الف) شناسائی شماره تلفن تماس گیرنده – استفاده از عملکرد تصدیق با ایجاد تماس برگشتی با تلفن گیرنده تماس توسط کارکرد تصدیق هویت گیرنده تماس [1]
ب) استفاده از ابزار هایی نظیر نرم افزار ضد ویروس
پ) بازنگری گزارش ردیابی ممیزی ارتباط در خصوص دسترسی غیر قانونی به یک کامپیوتر

۴-۱-۲-۲ خدمات سرویس ونگهداری از راه دور با استفاده از اینترنت

یک وسیله برای ارتباط اینتر نتی با یک آدرس IP ثابت جهانی در سایت HCF قرار می گیرد. محیط ارتباط اینترنتی توسط RSC آماده و خودش از طریق اینترنت به HCF متصل می شود.
این استاندارد فن آوری های بیشتری برای ارتباط و تصدیق کاربر بین HCF و RSC را طلب می کند، زیرا این ارتباط مشابه با ارتباط اینترنتی متداول است، نه مشابه با یک ارتباط یک به یک از طریق یک تلفن سوئیچ شده.
در این استاندارد مثال های زیر به وضوح تشریح می شوند:
الف) نصب یک فایر وال
ب) استفاده از ابزار ها ئی مانند نرم افزار ضد ویروس
پ) ارتباط از طریق VPN برای تصدیق مسیر ارتباط
ت) استفاده از روش های مختلف گواهی کاربر نظیر گذر واژه های یکبار مصرف، رمز گذاری گذر واژه و استفاده از گواهی های دیجیتالی

۴-۲ الزامات امنیتی خدمات سرویس و نگهداری از راه دور

۴-۲-۱ تدابیر امنیتی در عملیات خدمات سرویس ونگهداری از راه دور

مقررات موجود، هم به منظور اداره ایمن سیستم و هم برای امنیت اطلاعات شخصی افراد بصورت مشترک مورد استفاده قرار می گیرند.
در این استاندارد مثال ها ئی از این مقررات شرح داده می شوند:
الف) مقرراتی در خصوص اپراتور RSC
ب) تدابیر مقرراتی برای حذف افراد غیر مجاز از اجازه دسترسی به ترمینال های از راه دور RSC
پ) مقررات برای زمانی که ترمینال های RSC اضافه شده یا انتقال می یابند
ت) مقررات برای دسترسی از طریق ترمینال های همراه (سیار).

۴-۲-۲ قرار داد های بین HCF و RCS

مقررات زیر ممکن است برای موارد بروز حوادث غیر منتظره برقرار گردند:
الف) مقررات برای توصیف مسئولیت بین HCF و RSC

1-CallerID specification certification function

ب) نتایج حاصل از قرار داد ها در خصوص راز داری اطلاعات
راه کار های گوناگونی برای فراهم نمودن اقدامات امنیتی در یک RMS وجود دارد. هر تامین کننده RMS با استفاده از این راه کار ها همراه با مقررات اصلی، امنیت را حفظ می کند.
در هر حال، این استاندارد با این واقعیت روبروست که هزینه تامین امنیت رو به افزایش است و حفظ سطح امنیت برای HCF در آینده مشکل تر خواهد شد زیرا روش های استفاده شده توسط تامین کنندگان RMS متفاوت هستند.

۴-۲-۳ حفظ اطلاعات شخصی و خدمات سرویس ونگهداری از راه دور

۴-۲-۳-۱ حفظ حریم اطلاعات سلامت در سازمان های حفظ سلامت

به دلیل قوانین موجود ناظر بر حفاظت از حریم خصوصی، مدیریت راز داری اطلاعات شخصی، از عهده پزشکان ساقط و به خود بیماران انتقال یافته است.
سازمان های حفظ سلامت برای تشریح ریسک های راز داری اطلاعات شخصی برای بیمار، و اطمینان از اینکه متخصصین حفظ سلامت از اطلاعات سلامت (در خارج از حوزه ای که بدان منظور جمع آوری شده اند) استفاده نمی کنند، نیازمند مدیریت اطلاعات شخصی می باشند.
از این رو که اطلاعات پزشکی بطور اخص یک نوع مهم از اطلاعات شخصی می باشند، بایستی به دقت و با امنیت کافی نگهداری شوند.

۴-۲-۳-۲ مسئولیت حفظ حریم اطلاعات شخصی و اقدامات مرتبط

مقررات HIPAA[1] آمریکا الزام می نماید که سازمان های حفظ سلامت، فردی را به عنوان "مسئول مدیریت اطلاعات" تعیین و مسئولیت افشای اطلاعات از سازمان حفظ سلامت را صرفنظر از دلیل آن را به عهده بگیرند.
در ژاپن، خطوط راهنما برای حفاظت از اطلاعات خصوصی در شاخه پزشکی، مسئولیت حفظ اطلاعات شخصی را به سازمان حفظ سلامت واگذار کرده و الزام نموده است فردی را برای حفاظت از اطلاعات شخصی در سازمان حفظ سلامت منصوب نمایند تا این مسئولیت را به انجام برساند. خود سازمان های حفظ سلامت بایستی اطلاعات را مدیریت نمایند.
به هر جهت ، این استاندارد مواردی را یافته است که در آن ها سازمان های حفظ سلامت، سیستم های مدیریت اطلاعات پزشکی را بطور کامل به تامین کنندگان RMS وسایل پزشکی و سیستم های اطلاعات پزشکی واگذار کرده اند. ممکن است با توجه به این که سازمان های حفظ سلامت اطلاعات را مدیریت می کنند، مدیریت یک بحران بطور مناسب توسط افراد منصوب شده دشوار باشد و بدین دلیل مدیریت اطلاعات بطور کامل به عهده تامین کنندگان RMS واگذار شده است.

1-The health insurance portability and accountability Act

در هر صورت، در مواردی که حوادثی منجر به افشای اطلاعات و سایر موارد می شود این سوال ممکن است مطرح شود که یک تامین کننده RMS یا یک مرکز حفظ سلامت چه کسی را باید مسئول بداند؟ برای حل مشکل، این استاندارد نشان می دهد که بهتر آن است که برای اطمینان از مطابقت داشتن با همه قوانین در تمام حوزه های ذیربط قانونی، سیستم مدیریت اطلاعات سازمان حفظ سلامت برای ارزیابی اثر بخش بودن سیستم حفظ اطلاعات شخصی، مورد بازنگری قرار گیرد.

۴-۲-۳-۳ همزیستی RMS با حفاظت از اطلاعات شخصی

برای حفاظت مناسب از اطلاعات شخصی، همان طور که در پاراگراف فوق تشریح شده است، سازمان های حفظ سلامت باید تدابیر امنیتی متناسب با مسئولیت سازمان حفظ سلامت را اتخاذ نمایند.

در حال حاضر، سازمان های حفظ سلامت بطور عمده قواعد مدیریت مرکز پزشکی را تامین، اقداماتی برای مدیریت مناسب را پایه گذاری، تدابیر امنیتی برای سیستم های اطلاعات را مستقر و اقدامات فنی برای حفظ اطلاعات شخصی را استقرار می دهند.

بطور اخص، در مورد امنیت شبکه، بسیاری از سازمان های حفظ سلامت، تدابیر اتخاذ شده در راستای خط مشی امنیتی خود را با اقداماتی مانند " ارتباط با یک شبکه خارجی مجاز نمی باشد " و " از VPN استفاده شود" و غیره را در برابر هکر های خارجی که سعی دارند از طریق اینترنت به اطلاعات دست یابند، به عنوان حربه دفاعی بر گزیده اند. اما، حتی اگر اقدامات پیشگیرانه یک سازمان حفظ سلامت، در برابر هجوم هکر ها تا حد قابل قبولی بی نقص باشد، RMS تنها مسیری بازی است که دسترسی از خارج را ممکن می سازد.

دسترسی کارکنان یک تامین کننده RMS به سیستم، از طریق خط RMS به عنوان یکی از امکانات ضروری برای تامین پاسخ گوئی و راه اندازی فوری در نظر گرفته می شود.

سیستم خدمات نگهداری از راه دور هم برای سازمان های حفظ سلامت و هم برای تامین کنندگان RMS فوایدی دارد و در نتیجه حتی بعد از انتشار و تایید قوانین و مقررات ناظر بر حفظ اطلاعات سلامت شخصی، یکی از خدمات ضروری محسوب می شود.

برای استفاده ایمن و مسئولانه از RMS ، سازمان های حفظ سلامت باید RMS را بدرستی درک نموده، یک قرار داد مناسب منعقد، و تدابیر فنی امنیت اطلاعات و اقدامات عملیاتی را مستقر نمایند. مهم است که مرز مسئولیت ها بین یک سازمان حفظ سلامت و تامین کنندگان RMS شفاف سازی شود، و یک ساز و کار ایمن قابل ارزیابی به منظور تضمین حفاظت از اطلاعات سلامت شخصی، برای این شفاف سازی به شیوه ای مناسب ساختار بندی گردد . هم سازمان حفظ سلامت و هم تامین کنندگان RMS باید همه تعهدات را بدرستی تشخیص داده و RMS مناسب را تحت توافق نامه متقابل به خدمت گیرند.

۴-۳ نقش مرکز خدمات از راه دور و سازمان حفظ سلامت

هر گاه HCF با عقد قرار داد نگهداریبا تامین کنندگان RMS، برای امنیت اطلاعات خود به تامین کننده RMS اعتماد کرده باشد، امنیت مورد نظر تحت نظارت و مسئولیت هر تامین کننده استقرار می یابد.

موارد زیر اتفاق می افتد :

- هیچ گونه اظهاریه ای برای شخص ثالث وجود ندارد که ثابت کند که تامین کننده RMS تدابیر امنیتی کافی را اتخاذ نموده است؛
- HCF تدابیر مدیریتی در اقدامات امنیتی را هم ارز اقدامات تکنولوژیک لحاظ نکرده است؛
- HCF به حد کفایت توالی وقایع را بعد از این که یک حادثه رخ داده، بررسی نکرده است؛
- HCF تهدید های عمده نظیر ویروس های کامپیوتری را آزمون نکرده است.

مفاد قانونی ناظر بر حفاظت اطلاعات پزشکی شخصی، HCF ها را ملزم می کند که مسئولیت امنیت اطلاعات پزشکی اشخاص را به عهده بگیرند، همچنین HCF ملزم به قبول مسئولیت برای حفظ امنیت RMS است. بنابر این، این استاندارد نقش تامین کنندگانHCF و RMS را تشریح می کند. استقرار امنیت در RMS از وظایف تامین کننده RMS است، زیرا فقط تامین کننده RMS می تواند عملیات RMS را برای سیستم اطلاعات پزشکی مستقر نماید. تامین کنندگان RMS باید توجه داشته باشند که استقرار سیستم با فن آوری های امنیتی متفاوت، گسترش RMS را محدود می کند.

تامین کنندگان می توانند برای فراهم کردن نقطه دسترسی برای هر RMS، مدیریت امنیت پیچیده ای را ایجاد نمایند. این گونه مدیریت پیچیده، خلاء امنیتی را بارز می کند. بنابر این هر تامین کننده RMS نیازمند اخذ و استقرار فن آوری امنیتی استاندارد و فن آوری های مورد استفاده در سطح وسیع می باشد. تدابیر مدیریتی و فن آوری مهم هستند. این تدابیر هم برای HCF و هم برای RSC ضروری می باشند. یک سیستم مدیریت امنیت، اطلاعات جاری را بر اساس یک استاندارد بین المللی نظیر ISO / IEC 27001 که استقرار یک سیاست امنیتی را حمایت می کند، مستندمی نماید. سپس آن ها باید در خصوص نحوه ارتباط با خط مشی امنیت اطلاعات مورد مقایسه قرار گیرند؛ همچنین مهم است که حد اقل ایمنی قابل حصول در یک استاندارد امنیتی در RMS را مشخص نمایند. HCF، تصمیم گیری و انجام اقدامات بر اساس خط مشی امنیتی خود و انجام آزمایشات و ارزیابی خط مشی امنیتی و رویداد های مرتبط با اقدامات امنیتی در RMS که توسط تامین کننده RMS مشخص شده است را به انجام می رساند. سپس HCF با تامین کننده RMS در خصوص توافق بر روی عملیات و راز داری، قرار داد می بندد و در نتیجه امنیت در RMS تضمین می گردد.

۵ مواردی از خدمات نگهداری از راه دور که مورد استفاده قرار گرفته اند

۵-۱ مقدمه

این استاندارد سه مورد نوعی از خدمات نگهداری از راه دور استفاده شده که به عنوان مدل برای سایت های عملیاتی پایه در نظر گرفته شده اند را استخراج کرده است.

الف) رفع اشکال قطع منبع تغذیه

در موارد قطع شدن منبع تغذیه تجهیزات در محل HCF، و در پاسخ به یک درخواست از مرکز HCF، عملیات نگهداری از طریق دسترسی به وسایل مورد نظر از محل RSC انجام می گیرد.

ب) نگهداریبرنامه ریزی شده

عملیات نگهداریبرنامه ریزی شده از محل RSC بوسیله جلب موافقت از مرکز HCF انجام می شود. این روش ممکن است سبب دسترسی دوره ای به وسایل مورد نظر در HCF گردد.

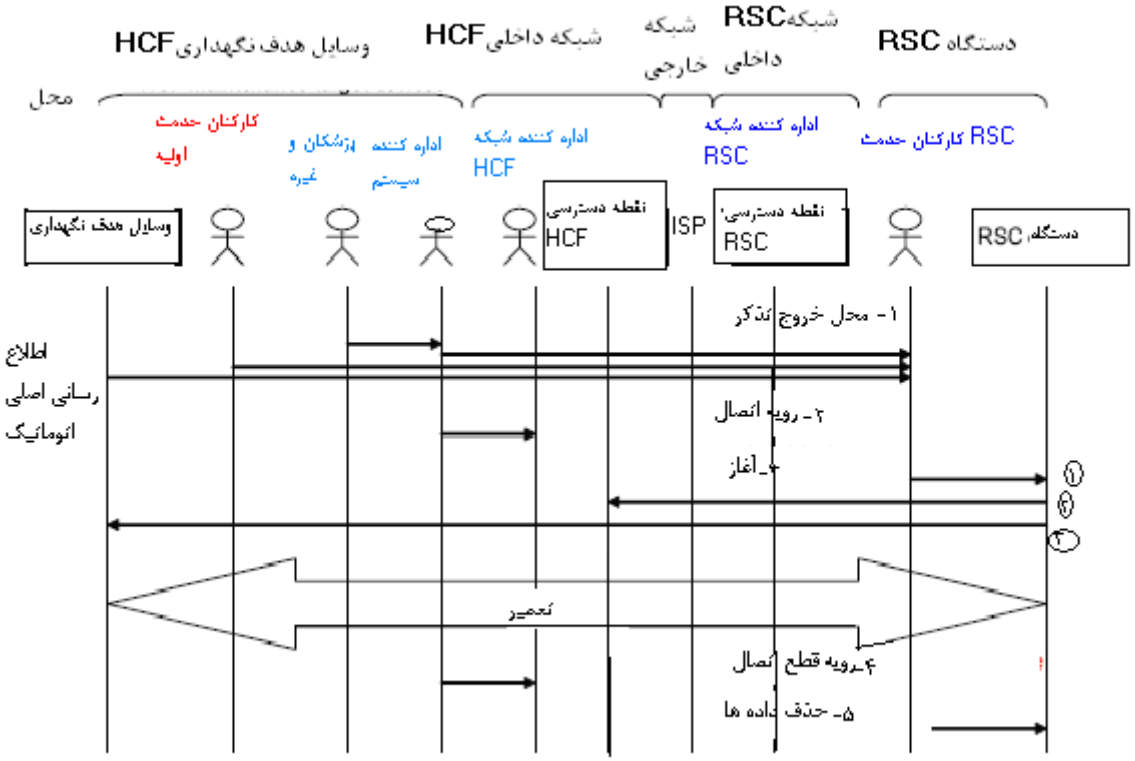
پ) به روز رسانی نرم افزار

به روز رسانی نرم افزار وسایل مورد نظر در مرکز HCF، از طریق دسترسی به آن ها از محل RSC انجام می گیرد.

۲-۵

رفع اشکال قطع منبع تغذیه

گردش کار رفع اشکال قطع منبع تغذیه در شکل ۲ آمده است.



شکل ۲- گردش کار رفع اشکال قطع منبع تغذیه

مراحل کار به شرح زیر است :

الف) RSC بوسیله HCF مطلع می شود که مشکل رخ داده است (این کار می تواند با یک نامه ارسالی توسط پست الکترونیک اتوماتیک انجام شود).

ب) RSC درخواست اتصال به شبکه برای RMS را برای HCF ارسال می کند.

پ) RSC مقدمات اتصال به شبکه را به انجام می رساند.

ت) کارکنان خدمات RSC، بازرسی، رفع عیب و اعلام خاتمه را از طریق شبکه ارتباطی به شرح زیر انجام می دهند:

۱) استقرار یک برنامه بازرسی خود کار؛

۲) جمع آوری اطلاعات مرتبط از وسایل مورد نظرشامل:

- گزارش عملیات؛
- داده های تصویری؛
- فایل های پیکر بندی / پیکر بندی سیستم؛
- محتویات پایگاه داده (بانک اطلاعاتی) ؛

۳) بررسی مشکل؛

۴) چنانچه منشاء مشکل در نرم افزار باشد، تغییر[1] یا بروز رسانی تجهیزات مورد نظربه شرح زیر انجام میگیرد:

) تغییر فایل های پیکر بندی؛

) به روز رسانی نرم افزار؛

) بازیابی داده ها؛

۵) چنانچه منشاء مشکل در سخت افزار باشد، تماس با کارکنان اصلی واحد خدمات برای تعویض قطعات آسیب دیده؛

۶) انجام بازرسی پس از تعمیر.

ت) RSC نتیجه کار را به HCF گزارش می کند.

ث) RSC اتصال شبکه به RMS را قطع می کند.

ج) RSC از HCF درخواست قطع شبکه به RMS را می کند.

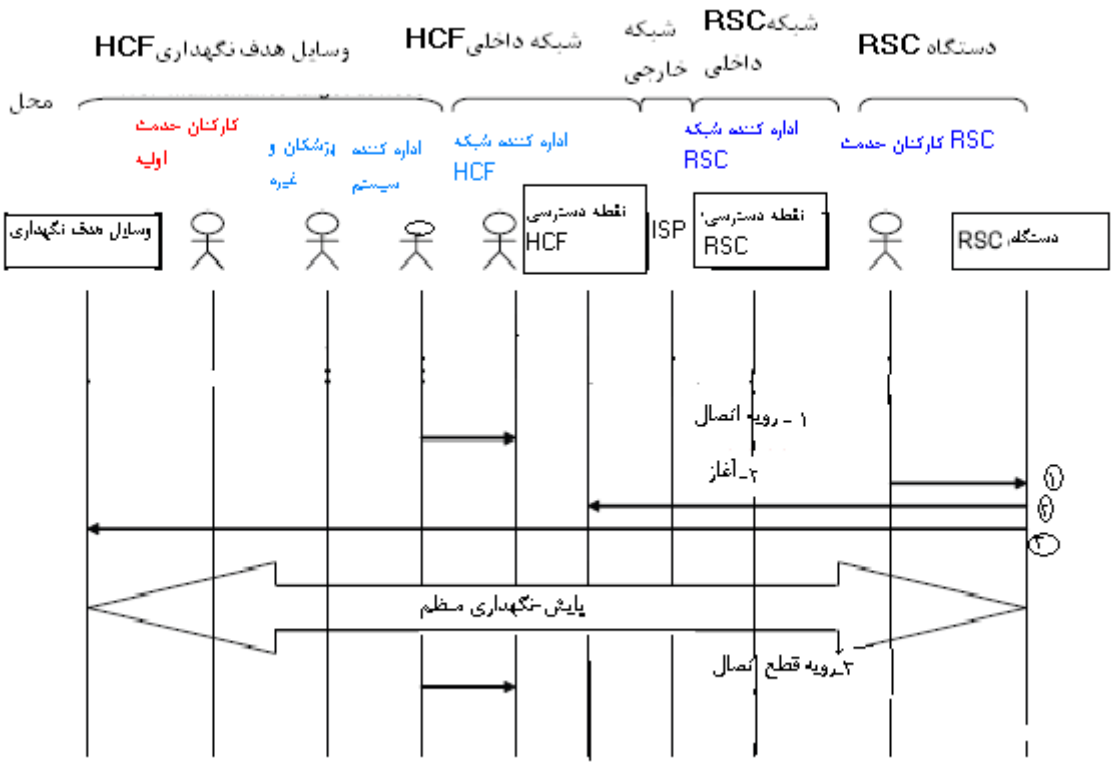
چ) چنانچه RSC، PHI را انتقال داده باشد، RSC همه کپی های PHI موجود در سایت خود را پاک می کند.

۳-۵

نگهداری برنامه ریزی شده

گردش کار در مورد نگهداری برنامه ریزی شده در شکل ۳ آمده است.

1-Modification



شکل ۳ – گردش کار در مورد سرویس و نگهداری برنامه ریزی شده

مراحل کار به شرح زیر است :

الف) RSC درخواست اتصال شبکه برای RMS را برای HCF ارسال می کند.

ب) RSC مقدمات اتصال به شبکه را به انجام می رساند.

پ) کارکنان خدمات RSC بازرسی برنامه ریزی شده را از طریق شبکه ارتباطی به شرح زیر انجام می دهند.

۱) استقرار یک برنامه بازرسی خود کار؛

۲) بررسی گزارشات؛

۳) بررسی کیفیت تصویر (صحت)؛

۴) جمع آوری اطلاعات عملیات؛

ت) RSC نتیجه کار را به HCF گزارش می کند.

ث) RSCاتصال شبکه برای RMS را قطع می کند.

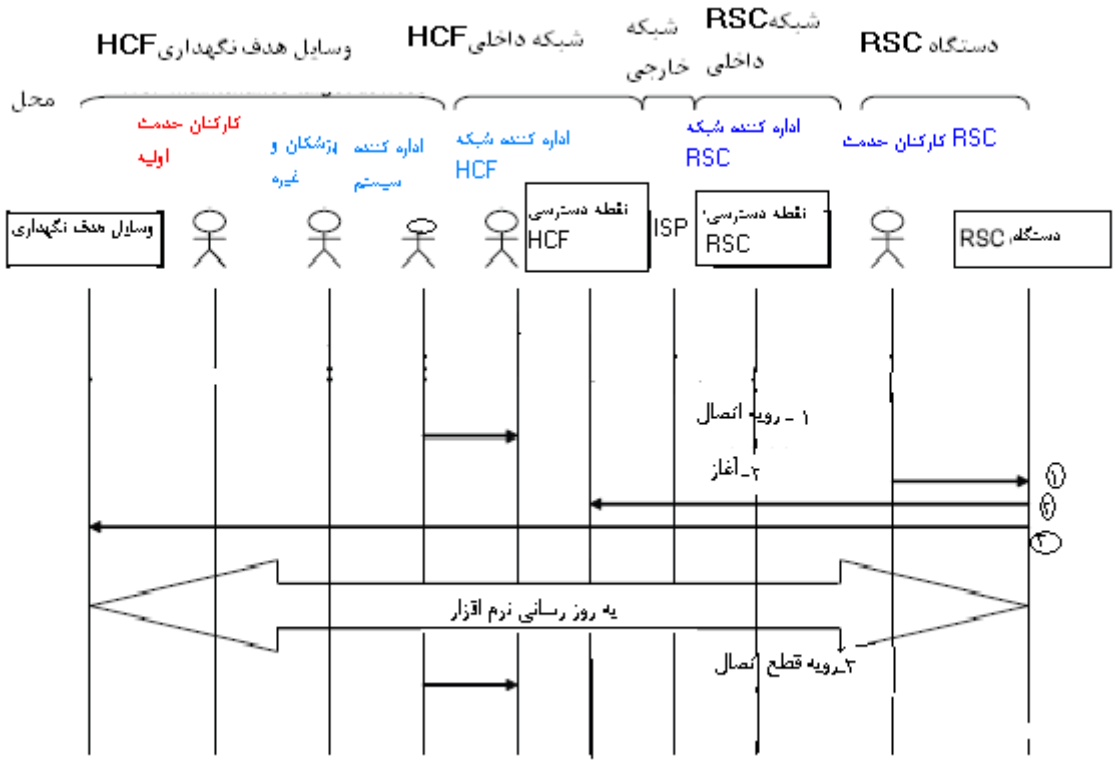
ج) RSC از HCF درخواست قطع شبکه برای RMS را می کند.

چ) چنانچه RSC، PHI را انتقال باشد، RSC همه کپی های PHI موجود در سایت خود را پاک می کند.

۴-۵

به روز رسانی نرم افزار

گردش کار به روز رسانی نرم افزار در شکل ۴ آمده است.



شکل – ۴ گردش کار به روز رسانی نرم افزار

مراحل کار به شرح زیر است:

الف) RSC به منظور RMS از HCF درخواست اتصال به شبکه را ارسال می کند.

ب) RSC مقدمات اتصال به شبکه را فراهم می کند.

پ) کارکنان خدمات RSC نرم افزار را از طریق شبکه به ترتیب زیر به روز می کنند:

۱) جایگزین کردن نرم افزار؛

۲) تغییر دادن پیکربندی؛

۳) تصدیق عملیات کار کردی.

ت) RSCگزارش نتیجه کار را به HCF می دهد.

ث) RSC اتصال شبکه به RMS را قطع می کند.

ج) RSC از HCF قطع شبکه برای RMS را درخواست می کند.

چ) چنانچه RSC، PHI را انتقال داده باشد، RSC همه کپی های PHI در سایت خود را پاک می کند.

۶ تحلیل ریسک

۱-۶

کلیات

در این بند، یک مورد از تحلیل ریسک بر اساس موارد استفاده شده در بند ۵ توضیح داده شده است.

۶-۲

معیار های تحلیل ریسک

۶-۲-۱

خط مشی

خط مشی سازمان، اداره ثبت اطلاعات را که مسئول این کار در سازمان حفظ سلامت است ملزم می کند تا تدابیر لازم در خصوص امنیت و ریسک محتمل برای سازمان حفظ سلامت را بر اساس روش های HIPAA اتخاذ نماید. بنابر این ضروری است که ریسک پیش بینی شود و برای تبادل اطلاعات توسط افراد خارج از سازمان راه کاری اندیشه شود.

این تحلیل توسط HCF به عنوان یک سند مکمل یا یک راهنما در قرار داد با RSC گنجانده می شود. برای هر یک از سازمان های حفظ سلامت افزوده شده، انجام این تحلیل توسط مدیریت ضروریست.

۶-۲-۲ دسته بندی سایت

دسته بندی سایت به شرح زیر انجام شده است

- تجهیزات تحت خدمات RSC
- شبکه داخلی RSC
- شبکه خارجی
- شبکه داخلی HCF
- وسایل مورد نظرHCF

۶-۲-۳ نمایه حفاظت

نمایه حفاظت به شرح زیر است:

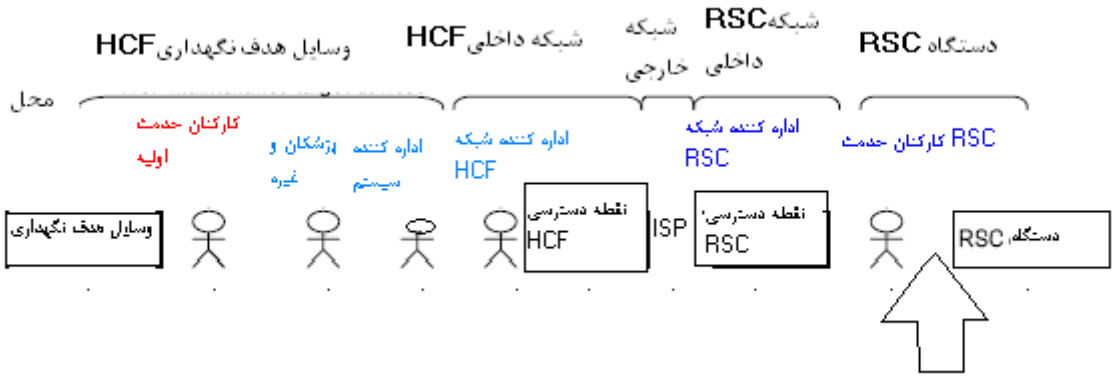
- راز داری : دزدکی دید زدن / خیانت در امانت، ورود غیر مجاز به شبکه/ و روش های فریب دادن و آزمون و خطا
- یکپارچگی: تحریف، جایگزین کردن، جعل و عدم ممانعت از موارد غیر مجاز
- در دسترس بودن: اشکال تجهیزات، حادثه ناگوار، نبود ارائه خدمات به دلیل قطعی کابل ارتباطی یا سر باز زدن از انجام کار

پیوست الف

(اطلاعاتی)

یک مثال از نتیجه تحلیل ریسک در مورد خدمات نگهداری از راه دور

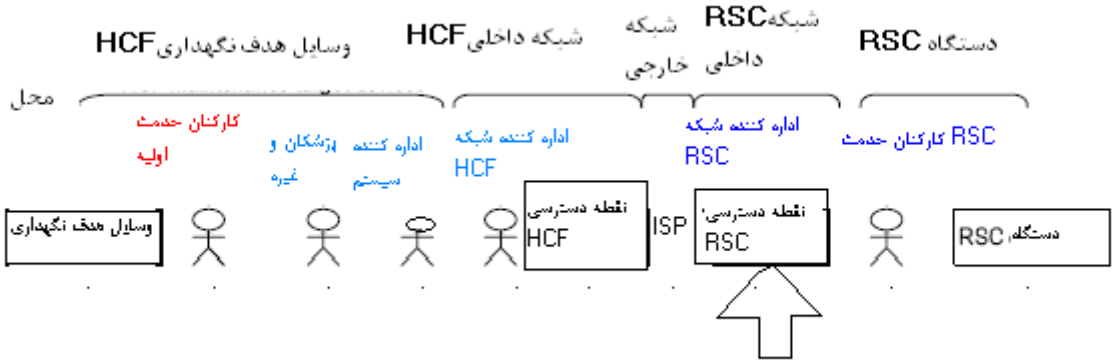
الف-۱ ذخائر و تهدید ها



جدول الف ۱- ذخائر و تهدید ها

ذخائر	شماره	تهدید(C=رازداری، I= یکپارچگی، A = قابلیت سترسی)
اطلاعات ذخیره شده PHI بر روی حافظه ، دیسک و صفحه نمایش	۱۱	در معرض دید قرار گرفتن (C) با پاک کردن خطا در سایت (C)، دزدکی دید زدن (C)/سرقت (C)، ورود غیر مجاز به تجهیزات RSC (C) / فریب دادن (C)
	۱۲	در معرض دید قرار گرفتن (C) سرقت از طریق مسیر (C) ورود غیر مجاز به تجهیزات RSC (C) / فریب دادن (C)
یاد داشت برداری و چاپ اطلاعات PHI بالا	۱۳	در معرض دید قرار گرفتن (C) دیدزدن اسناد بایگانی تعمیرات (C) با بیرون بردن (C)
محیط پشتیبانی از اطلاعات PHI بالا	۱۴	در معرض دید قرار گرفتن (C) با بیرون بردن حافظه برای تعمیر
نرم افزار رسیدگی کننده به اطلاعات PHI	۱۵	در معرض دید قرار گرفتن (C) با سرقت یا نصب پنهانی نرم افزار مخصوص سرقت اطلاعات (I)
نرم افزار مرتبط با اطلاعات PHI	۱۶	در معرض دید قرار گرفتن (C) با بیرون بردن (C) رشوه (C) نشت تشعشعات الکترو مغناطیس (C)
	۱۷	عدم امکان ارائه خدمات (A) به علت اشکال (C) حادثه (A) آسیب (A)
تجهیزات مرتبط با اطلاعات PHI*	۱۸	عدم امکان ارائه خدمات (A) به علت اشکال (C) حادثه (A) آسیب (A)
کاربر های رسیدگی کننده به اطلاعات PHI	۱۹	افشا کردن با رشوه (C) اشکال در خدمت (A) با ورودی نادرست (I) / حذف اشکال از سایت (A)
رمز گذاری الگوریتم ، کلیدها و روش توزیع کلیدی	۱الف	در معرض دید قرار گرفتن (C) با رمز گشایی داده های رمز گذاری شده (C)
*به تاسیسات منبع تغذیه/ قطع جریان برق اشاره دارد. در هر حال تجهیزات شبکه را شامل نمی شود.		

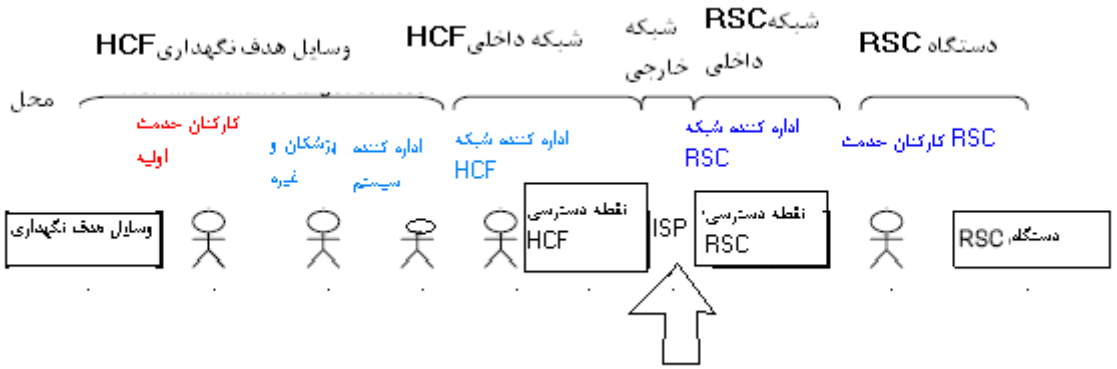
الف-۲ ذخائر و تهدید ها (محل : شبکه داخلی RSC)



جدول الف۲- ذخایر ، تهدید ها و اقدامات پیشگیرانه در محل شبکه داخلی RSC

ذخائر	شماره	تهدید(C=رازداری،I= تمامیت، =Aقابلیت در دسترس بودن)	با اقدامات پیشگیرانه با VPN
اطلاعات PHI بر روی شبکه داخلی RSC	۲۱	در معرض دید قرار گرفتن (C) دید زدن پنهانی مسیر (C) ورود غیر مجاز به تجهیزات شبکه RSC (C)/ فریب دادن (C) برقراری اتصال غیر مجاز (C)	برای این تهدید ات به جز مورد (A) قابلیت دسترسی جزئی است
یادداشت ها و مدارک چاپ شده از ردیابی ارتباطی اطلاعات فوق	۲۲	در معرض دید قرار گرفتن (C) دیدزدن مخفیانه صفحه مونیتور (C) بیرون بردن(C)	
محیط پشتیبان از ردیابی ارتباطی اطلاعات فوق	۲۳	در معرض دید قرار گرفتن (C) با بیرون بردن محیط ذخیره سازی مونیتور(C)	
نرم افزار تجهیزات شبکه	۲۴	در معرض دید قرار گرفتن (C) توسط سرقت یا نصب مخفیانه برنامه سرقت اطلاعات (I)	
تجهیزات شبکه	۲۵	در معرض دید قرار گرفتن (C) با بیرون بردن(C) رشوه (C) نشت تشعشع الکترو مغناطیسی (C)	
	۲۶	عدم امکان ارائه خدمات(A) بدلیل خطا (A)حادثه(A) آسیب (A)	
تسهیلات محیطی برای تجهیزات شبکه *	۲۷	عدم امکان ارائه خدمات (A) بدلیل خطا(A) حادثه (A) آسیب (A) قطع شدن کابل(A)	
کاربران تجهیزات شبکه	۲۸	در معرض دید قرار دادن با رشوه (C) در معرض دید قرار گرفتن (C) با تنظیم نادرست(C)	
الگوریتم رمز گذاری شده، کلید ها، روش توزیع کلیدی	۲۹	در معرض دید قرار گرفتن (C) با رمز گشایی داده رمز گذاری شده (C)	
*به تاسیسات منبع تغذیه/ قطع جریان برق اشاره دارد.			

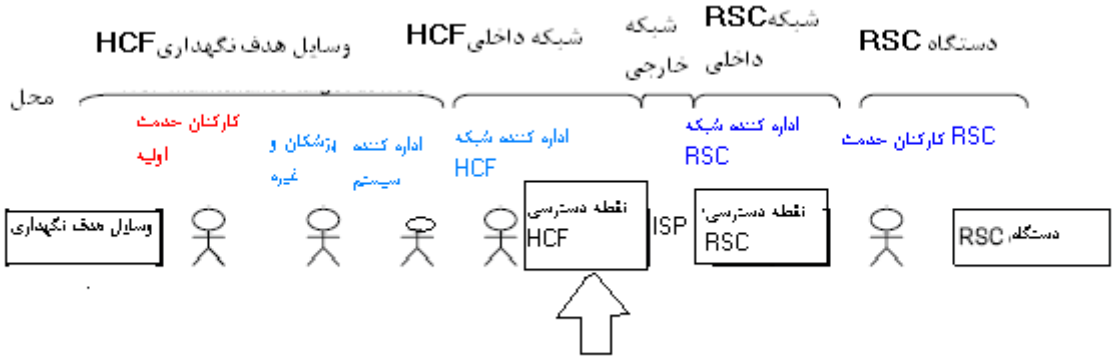
الف ۳- ذخائر و تهدید ها (محل : شبکه خارجی)



جدول الف۳- ذخایر و تهدید ها در محل شبکه خارجی

ذخائر	شماره	تهدید (C=رازداری،I= یکپارچگی A = قابلیت دسترسی) فرض شده است که بر روی VPN اقدامات پیشگیرانه انجام گرفته است. تهدید ها به جز برای قابلیت دسترسی (A) جزئی است
اطلاعات PHI بر روی شبکه خارجی	۳۱	جزئی
یاد داشت ها و مدارک چاپی از ردیابی ارتباطی اطلاعات فوق	۳۲	جزئی
محیط پشتیبانی از ردیابی ارتباطی اطلاعات فوق	۳۳	جزئی
نرم افزار تجهیزات شبکه	۳۴	جزئی
تجهیزات شبکه	۳۵	جزئی
	۳۶	ارائه خدمات ممکن نیست (A) بدلیل خطا (A) حادثه(A) آسیب(A)
تسهیلات محیطی تجهیزات شبکه *	۳۷	ارائه خدمات ممکن نیست (A) بدلیل خطا (A) حادثه(A) آسیب (A) قطع شدن کابل (A)
کاربران تجهیزات شبکه	۳۸	جزئی
الگوریتم های کد گذاری شده، کلید ها، روش توزیع کلیدی	۳۹	در معرض دید قرار گرفتن (C) با کد گشایی از داده های کد گذاری شده (C)
*به تاسیسات منبع تغذیه/ قطع جریان برق اشاره دارد.		

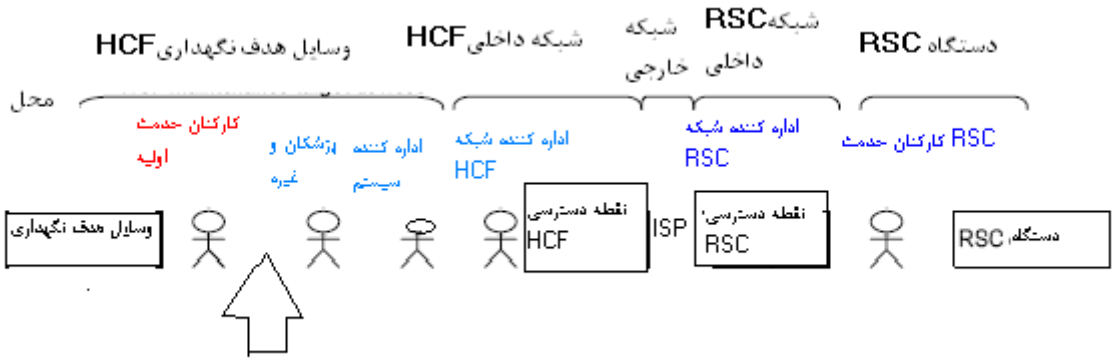
الف- ۴ ذخائر و تهدید ها (محل : شبکه داخلی HCF)



جدول الف۴- ذخایر و تهدید ها در محل شبکه داخلی HCF

ذخائر	شماره	تهدید (C=رازداری،I= یکپارچگی ، A = قابلیت دسترسی)
اطلاعات PHI برروی شبکه داخلی HCF	۴۱	در معرض دید قرار گرفتن (C) دیدن مخفیانه مسیر (C)ورود غیر مجاز به تجهیزات شبکه HCF(C) / فریب دادن (C) برقراری اتصال غیر مجاز(C)
یاد داشت ها و مدارک چاپی از ردیابی ارتباط اطلاعات فوق	۴۲	در معرض دید قرار گرفتن (C) دیدزدن مخفیانه صفحه مونیتور(C) با بیرون بردن(C)
محیط پشتیبانی از ردیابی ارتباط اطلاعات فوق	۴۳	در معرض دید قرار گرفتن (C) با بیرون بردن حافظه مونیتور(C)
نرم افزار تجهیزات شبکه	۴۴	در معرض دید قرار گرفتن (C) سرقت یا نصب مخفیانه برنامه سرقت اطلاعات
تجهیزات شبکه	۴۵	در معرض دید قرار گرفتن (C) بیرون بردن (C) رشوه (C) نشت تشعشعات الکترو مغناطیسی(C)
	۴۶	عدم امکان ارائه خدمات(A) بدلیل خطا (A)حادثه (A) آسیب(A)
تسهیلات محیطی تجهیزات شبکه	۴۷	عدم امکان ارائه خدمات(A) بدلیل خطا (A)حادثه (A) آسیب (A) قطع شدن کابل(A)
کاربران تجهیزات شبکه	۴۸	در معرض دید قرار دادن با رشوه (C) در معرض دید قرار گرفتن(C) تنظیم نادرست(C)

الف-۵ ذخائر و تهدید ها (محل : وسایل هدف برای نگهداری HCF)



جدول الف۵- ذخایرو تهدید ها در محل وسایل هدف برای نگهداری HCF

ذخائر	شماره	تهدید (C=رازداری، I = یکپارچگی ، A = قابلیت دسترسی)
اطلاعات PHI ذخیره شده بر روی حافظه ، دیسک و صفحه نمایش	۵۱	در معرض دید قرار گرفتن (C) ساخت (I) با حذف خطا از روی خط (C) مخفیانه دید زدن (C) / دزدی (C) ورود غیر مجاز به وسایل هدف سرویس و نگهداری (C) / فریب دادن (C) تعویض (I)
	۵۲	در معرض دید قرار گرفتن (C) ساخت (I) با سرقت از مسیر (C) ورود غیر مجاز به وسایل هدف نگهداری (C) / فریب دادن (C) تعویض(I)
یاد داشت ها و چاپ اطلاعات PHI بالا*	۵۳	در معرض دید قرار گرفتن (C) ساخت (I) با دید زدن یادداشت های ضبط شده عملیات (C) دید زدن پنهانی (C) تعویض(I)
محیط پشتیبانی از اطلاعات PHI بالا **	۵۴	در معرض دید قرار گرفتن (C) ساخت (I) با خارج کردن حافظه اطلاعات عملیاتی (C) تعویض(I)
نرم افزار مرتبط با اطلاعات PHI	۵۵	در معرض دید قرار گرفتن (C) سرقت / نصب پنهانی برنامه سرقت اطلاعات (I)
تجهیزات مرتبط با اطلاعات PHI	۵۶	در معرض دید قرار گرفتن (C) ساخت (I) با تعویض (I) خارج کردن (C) رشوه (C) نشت تشعشعات الکترو مغناطیسی (C)
تجهیزات مرتبط با اطلاعات PHI	۵۷	ارائه خدمت امکان پذیر نیست (A) بدلیل خطا (A)حادثه (A) آسیب(A)
تسهیلات محیطی تجهیزات مرتبط با اطلاعات PHI***	۵۸	ارائه خدمت امکان پذیر نیست (A) بدلیل خطا (A)حادثه (A) صدمه(A)
کاربران رسیدگی کننده به اطلاعات PHI	۵۹	در معرض دید قرار دادن با رشوه (C) ورودی نادرست (I) خدمات ناقص یا ناکارآمد (A) با حذف نادرست(A)

* اسناد و محیط ذخیره سازی وارد شده مورد نظر نیست.

**کنترل ورودی اطاق از مشخصه های بیمارستان فرض نشده است.

*** به تاسیسات منبع تغذیه/ قطع جریان برق اشاره دارد.

کتاب نامه

[1] ISO/IEC Guide 73:2002, *Risk management — Vocabulary — Guidelines for use in standards*

[2] ISO/IEC 9797-1:1999, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*

[3] ISO/IEC 13335-1:2004, *Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management*

[4] ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements*

[5] ISO/IEC 27002:2005, *Information technology — Security techniques — Code of practice for information security management*