

شورای اجرایی (عالی) فناوری اطلاعات کشور
کمیسیون توسعه دولت الکترونیکی

چارچوب معماری سازمانی ایران

معماری مربع امنیت استانداردهای امنیتی حوزه سلامت

پیشگفتار

سلامت الکترونیک^۱ یک زمینه نوظهور از برخورد انفورماتیک، پزشکی، بهداشت عمومی و تجارت است که از طریق شبکه جهانی وب و تکنولوژی های مرتبط با آن ارتقا و تکامل می یابد. سلامت الکترونیک را نه تنها به عنوان یک توسعه فنی بلکه به عنوان حالتی روحی، طرز تفکر و یک حرکت عمومی جهانی می توان توصیف کرد. برای توصیف واژه سلامت الکترونیک باید از فناوری اطلاعات و ارتباطات در بخش سلامت بهره برد. اطلاعات دیجیتالی در بخش سلامت و بهداشت برای مقاصد بالینی و آموزشی و مدیریتی از طریق الکترونیکی، انتقال ذخیره و بازیابی می شود.

واژه e-Health ابتدا در دهه ۹۰ میلادی کلمه ای عمومی بود و به تمام مسائل مشترک میان کامپیوتر و پزشکی اطلاق می شد. این کلمه در ابتدا بیشتر به وسیله بخش صنعت و تجارت مورد استفاده واقع می شد و کاربرد علمی آن بسیار کم بود. در آن زمان تمام خدماتی که اینترنت برای سلامت جامعه می توانست ارائه دهد در این حوزه قرار می گرفت. به عنوان مثال شرکت اینتل از e-Health به عنوان تلاشی مشترک از سوی مسئولان بهداشت جهانی و فناوری یاد می کند، اما با گسترش نفوذ اینترنت در جوامع و افزایش گرایش کاربران به استفاده از اینترنت، سلامت دیجیتال نیز دچار تحولی عظیم شد و از کاربردی عمومی خارج شده و تبدیل به یک زیرشاخه از بهداشت عمومی شد.

در این حوزه از سلامت دیجیتال امکان تبادل اطلاعات و اسناد پزشکی میان مؤسسات بهداشتی و درمانی فراهم خواهد شد به نحوی که همواره از آخرین تغییرات دارویی، نسخه های درمانی، آموزش های پرستاری و مراقبتی و دیگر اطلاعات مورد نیاز آگاه شوند، بانک های اطلاعاتی این مؤسسات همواره به روز بوده و از آخرین تجربیات همکاران خود در هر گوشه از جهان می توانند استفاده کنند.

سلامت الکترونیکی الگوهای نوین ارتباطی میان پزشک و بیمار؛ پزشک و پزشک را ایجاد خواهد کرد و چالش ها، تهدیدها، تحولات و نیز فرصت های جدیدی از جنبه اخلاق را به وجود می آورد. از جمله این چالش ها بحث اخلاق پزشکی در درمان های آنلاین، محرمانه ماندن اطلاعات بیماران، محرمانه نگه داشتن مهارت های تخصصی پزشکان و نیز رضایت پزشک و بیمار در درمان است.

^۱ e-Health

با توجه به این شرایط ایجاد امنیت و حفظ حریم خصوصی در بخش سلامت از اهمیت ویژه‌ای برخوردار است که لازم به رسیدگی می‌باشد. در این راستا اسنادی تنظیم و منتشر گردیده که به تعدادی از مهم‌ترین آن‌ها در ادامه اشاره می‌گردد. لازم به ذکر است که مبحث امنیت در بخش سلامت موضوعی است که در هر کشور باید متناسب با سیاست‌ها و قوانین خاصی که در آن کشور بر این حوزه حاکم است مورد بررسی و مطالعه قرار بگیرد.

لیست استانداردهای امنیتی حوزه سلامت

شماره استاندارد	نام استاندارد
AUTO11-A2	IT Security of In Vitro Diagnostic Instruments and Software Systems; Approved Standard- second edition (2014)
	امنیت فناوری اطلاعات در ابزارهای تشخیصی آزمایشگاهی و سیستم‌های نرم‌افزاری
IEC 80001	Application of risk management for IT-networks incorporating medical devices (2010)
	کاربرد مدیریت ریسک برای دستگاه‌های پزشکی ادغام‌شده با شبکه‌های IT
ISO TR 17791	Health informatics -- Guidance on standards for enabling safety in health software (2013)
	اطلاعات سلامت- راهنمای استانداردهایی برای قابلیت ایمنی در نرم‌افزار سلامت
ISO 14971	Medical devices -- Application of risk management to medical devices (2007)
	دستگاه‌های پزشکی- کاربرد مدیریت ریسک در دستگاه‌های پزشکی
AAMI TIR57	Principles for medical device security—Risk management (2016)
	اصولی برای مدیریت ریسک امنیتی دستگاه‌های پزشکی
	The Privacy and Security Gaps in Health Information Exchanges (2011)
	شکاف‌های حریم خصوصی و امنیت در مبادلات اطلاعات سلامت

➤ **AUTO11-A2 - IT Security of In Vitro Diagnostic Instruments and Software Systems**

این سند یک چارچوب برای مسائل امنیت ارتباطات IT بین فروشندگان سیستم‌های تشخیص در شرایط آزمایشگاهی^۲ و سازمان‌های بهداشت و درمان فراهم می‌کند. چاپ دوم این استاندارد شامل تاکید بیشتری بر روی سیستم‌های رایانه و امنیت در سیستم‌های مراقبت‌های بهداشتی دارد. یک حمله سایبری می‌تواند تاثیر منفی بر بهره‌برداری از یک سیستم IVD، تحویل نتایج توسط یک سیستم IVD، نتایج تولیدشده توسط ابزار IVD و ایمنی اپراتور کنترل‌کننده ابزار IVD داشته باشد.

AUTO11-A2 راهنمایی که فروشندگان IVD برای حفاظت از محرمانگی، یکپارچگی و دسترس‌پذیری سیستم IVD خود نیاز دارند را فراهم می‌کند. نسخه دوم از AUTO11 استاندارد متناسب با فن‌آوری‌های جدیدی که پس از آخرین انتشار در سال ۲۰۰۶ پدید آمده‌اند، می‌باشد.

➤ **IEC 80001-1**

این سند به ترکیب دستگاه‌های پزشکی با فناوری شبکه برای رسیدن به منافع مطلوب (به عنوان مثال، قابلیت همکاری)، تعریف نقش‌ها، مسئولیت‌ها و فعالیت‌ها اذعان دارد و بیان می‌کند که مدیریت ریسک در شبکه‌های IT ترکیب‌شده با دستگاه‌های پزشکی برای رسیدگی به ایمنی، اثربخشی و امنیت داده‌ها و سیستم ضروری است. IEC 80001-1 سطح ریسک قابل‌قبولی را مشخص نمی‌کند. IEC 80001-1 پس از این که یک دستگاه پزشکی توسط یک سازمان مسئول تهیه می‌شود اعمال می‌گردد و در سراسر چرخه حیات شبکه‌های IT ترکیب‌شده با دستگاه‌های پزشکی به کار گرفته می‌شود.

IEC 80001-1 بر روی سازمان‌ها، تولیدکنندگان دستگاه‌های پزشکی و ارائه‌دهندگان فناوری‌های دیگر به منظور مدیریت ریسک دستگاه‌های پزشکی ترکیب‌شده با شبکه IT توسط سازمان مسئول

² in vitro diagnostic (IVD)

مشخص شده اعمال می‌شود. جهت پیاده‌سازی و به‌کارگیری این استاندارد یک سری از استانداردهای دیگر تنظیم شده است که در توضیحات تکمیلی بیان می‌شود.

توضیحات تکمیلی

➤ IEC TR 80001-2-1:2012

IEC / TR 80001-2-1، که یک گزارش فنی است، یک راهنمای گام به گام برای کمک به استفاده از مدیریت ریسک در هنگام ایجاد و یا تغییر یک شبکه IT پزشکی است. این سند مراحل، مثال‌ها و اطلاعاتی برای کمک به شناسایی و کنترل ریسک فراهم می‌کند. همه الزامات مربوطه در IEC 80001-1 به دیگر بند و زیربندهای استاندارد IEC 80001-1 پرداخته و لینک داده شده است. این گزارش فنی روی مدیریت ریسک عملی تمرکز دارد و برای ارایه یک طرح کامل و یا توضیح همه الزاماتی که در IEC 80001-1 مورد پوشش قرار گرفته است در نظر گرفته نشده است.

➤ IEC TR 80001-2-2:2012

IEC / TR 80001-2-2، یک گزارش فنی است، که یک چارچوب برای بیان قابلیت‌های امنیتی و خطرات ضروری برای مدیریت ریسک در دستگاه‌های پزشکی متصل به شبکه IT ایجاد می‌کند. این گزارش امنیتی یک مجموعه آموزنده از قابلیت‌های مربوط به امنیت مشترک و سطح بالا که برای درک نیازهای کاربر، نوع کنترل‌های امنیتی که باید در نظر گرفته شود و خطراتی که منجر به کنترل‌ها می‌شود، ارایه می‌دهد.

➤ IEC TR 80001-2-3:2012

IEC / TR 80001-2-3 یک گزارش فنی است، که از سازمان‌های ارایه‌دهنده بهداشت و درمان³ (HDO) برای مدیریت ریسک شبکه‌های IT پزشکی که با یک یا چند پیوند بی‌سیم ترکیب شده‌اند پشتیبانی می‌کنند. در این گزارش، به عنوان بخشی از IEC 80001، استفاده از دستگاه‌های پزشکی شبکه‌شده بی‌سیم در یک شبکه IT پزشکی مطرح می‌شود و تکنیک‌های عملی برای رسیدگی به الزامات خاص مدیریت ریسک در به کارگیری دستگاه‌های پزشکی بی‌سیم فعال به شیوه‌ای امن، ایمن و موثر ارایه می‌دهد. مخاطبان هدف برای

³ Health Delivery Organization (HDO)

این گزارش فنی بخش IT سازمان‌های ارائه‌دهنده بهداشت، بخش مهندسی پزشکی و بالینی، مدیران ریسک و افراد مسئول طراحی و بهره‌برداری از شبکه‌های IT بی‌سیم هستند.

➤ IEC TR 80001-2-4:2012

راهنمایی برای کمک به یک سازمان ارائه‌دهنده بهداشت و درمان برای انجام تعهدات خود به عنوان یک سازمان مسئول در به کارگیری IEC 80001-1 است، یک سازمان ارائه‌دهنده بهداشت و درمان شامل بیمارستان‌ها، مطب پزشکان، خانه‌های سالمندان و کلینیک‌ها می‌شود. به طور خاص، این راهنما کمک می‌کند تا این سازمان‌ها تاثیر IEC 80001-1 در سازمان و عملیات مدیریت ریسک خود برای ایجاد، نگهداری و حفظ شبکه IT پزشکی را ارزیابی کنند.

➤ IEC TR 80001-2-5:2014

IEC TR 80001-2-5 یک گزارش فنی است که تکنیک‌های هدایت‌کننده و عملی به سازمان‌ها، تولیدکنندگان دستگاه‌های پزشکی و ارائه‌دهندگان فناوری اطلاعات برای به کارگیری استاندارد IEC 80001-1 برای مدیریت ریسک سیستم‌های هشدار توزیع‌شده ارائه می‌دهد. این گزارش فنی برای انتقال شرایط هشدار بین منابع، تجمیع‌کننده‌ها و ارتباط برقرارکننده‌ها به کار گرفته می‌شود که در آن حداقل یک منبع یک دستگاه پزشکی است و حداقل یک مسیر ارتباطی با بهره‌گیری از فناوری شبکه پزشکی اجرا می‌شود. امنیت داده‌ها و سیستم‌ها برای مدیریت ریسک سیستم‌های هشدار توزیع‌شده مهم است.

➤ ISO TR 80001-2-6:2014

ISO / TR 80001-2-6 راهنمایی برای اجرای قراردادهای مسئولیت، که در IEC 80001-1 توضیح داده شده است به منظور ایجاد نقش‌ها و مسئولیت‌ها در میان سهامداران حوزه ادغام یک دستگاه پزشکی به یک شبکه IT برای حمایت از انطباق با استاندارد IEC 80001-1 فراهم می‌کند. سهامداران ممکن است شامل سازمان‌ها، ارائه‌دهندگان خدمات IT، تولیدکنندگان تجهیزات پزشکی باشند.

➤ ISO TR 80001-2-7:2015

ISO / TR 80001-2-7 راهنمایی برای ارائه‌دهندگان بهداشت و درمان برای انجام فرآیند خودارزیابی براساس

استاندارد IEC 80001-1 فراهم می‌کند.

➤ IEC/TR 80001-2-8:2016

یک گزارش فنی است که راهنمایی برای سازمان‌های ارائه‌دهنده مراقبت‌های بهداشتی و تولیدکنندگان دستگاه‌های پزشکی به منظور استفاده از چارچوب‌های مشخص شده در IEC TR 80001-2-2 فراهم می‌کند.

➤ IEC TR 80001-2-9:2017

IEC TR 80001-2-9 یک چارچوب امنیتی برقرار می‌کند و راهنمایی برای سازمان‌های ارائه‌دهنده مراقبت‌های بهداشتی و تولیدکنندگان دستگاه‌های پزشکی برای شناسایی، توسعه، تفسیر، به روزرسانی و حفظ موارد امنیتی برای دستگاه‌های پزشکی شبکه فراهم می‌کند.

➤ ISO TR 17791: Health informatics -- Guidance on standards for enabling safety in health software

ISO / TR 17791 راهنمایی برای شناسایی یک مجموعه منسجم از استانداردهای بین‌المللی مربوط به توسعه، اجرا و استفاده امن از نرم‌افزار سلامت فراهم می‌کند. چارچوب ارائه‌شده در این استاندارد، همراه با نگرانی از استانداردها در این چارچوب، توضیح استانداردهای مربوطه و چگونگی استفاده بهینه از آنها در این راهنما بیان شده‌اند.

➤ ISO 14971: Medical devices -- Application of risk management to medical devices

فرایندی برای یک تولیدکننده برای شناسایی خطرات مرتبط با دستگاه‌های پزشکی، از جمله دستگاه‌های پزشکی مورد استفاده در شرایط تشخیص آزمایشگاهی (IVD)، برای برآورد و ارزیابی خطرات مرتبط، کنترل این خطرات و نظارت بر اثربخشی این کنترل فراهم می‌کند. الزامات استاندارد ISO 14971 برای تمام مراحل چرخه حیات یک دستگاه پزشکی قابل اجرا می‌باشد.

➤ Principles for medical device security—Risk management

راهنمایی برای انجام مدیریت ریسک امنیت اطلاعات در یک دستگاه پزشکی با توجه به فرآیند "مدیریت ریسک ایمنی"^۴ ارائه شده در ISO 14971 فراهم می‌کند. این گزارش فنی نمای گسترده‌ای از مدیریت ریسک IEC 80001-1 را با خواص کلیدی ایمنی، اثربخشی و امنیت داده‌ها و سیستم‌ها ترکیب می‌کند و ضمایمی که جزئیات فرآیند و نمونه‌های گویایی را ارائه می‌کند، ایجاد کرده است.

➤ The Privacy and Security Gaps in Health Information Exchanges

این گزارش حریم خصوصی و امنیت را به چند بخش فرعی شکسته و مورد بحث قرار می‌دهد. برای حفاظت موثر از اطلاعات پزشکی افراد، تمام بخش‌ها باید در کنار یکدیگر مورد توجه قرار گیرند. در این سند مسائل مربوط به مدیریت امنیت، امنیت فنی و فیزیکی، مدیریت دسترسی، سلامت عمومی و حریم خصوصی مصرف‌کنندگان مورد بررسی قرار گرفته و راهنمایی‌هایی ارائه می‌گردد.

سازمان‌های حوزه سلامت

• موسسه استاندارد آزمایشگاهی و کلینیکی (CLSI)

در سال ۱۹۶۸، ۳۱ پزشک و دانشمند به نمایندگی از ۱۵ سازمان برای بهبود وضعیت رسیدگی به بیماران و توسعه یک فرآیند استانداردسازی گردهم جمع شدند و در سال ۱۹۷۷، CLSI توسط موسسه ملی استاندارد آمریکا (ANSI) به رسمیت شناخته شد. CLSI یک موسسه است که بدون منفعت و به صورت داوطلبانه به ترویج استاندارد مورد استفاده در آزمایشگاه‌ها و راهنماهایی برای

⁴ Safety Risk Management

سازمان‌های مراقبت پزشکی می‌پردازد. مأموریت این سازمان توسعه شیوه‌های کلینیکی و آزمایشگاهی و ترویج استفاده از آن‌ها در سراسر جهان می‌باشد.

- **انجمن پیشرفت ابزار دقیق پزشکی (AAMI)**

یک سازمان برای توسعه و استفاده ایمن و موثر از فناوری‌های پزشکی است که در سال ۱۹۶۵ توسط رابرت دی هال^۵ و رابرت جی آلن^۶ تأسیس شد. AAMI برای تنظیم مجموعه‌ای از استانداردهای ایمنی برای دستگاه‌های پزشکی در مرحله طراحی و استفاده از آن‌ها فعالیت می‌کند

⁵ Robert D. Hall

⁶ Robert J. Allen