NOBLE
COMPAÑÍA DE SEGUROS

1

LOS 10 PRINCIPALES PELIGROS TECNOLÓGICOS DEL SECTOR SALUD PARA EL 2015 *

Dr. Fabián Vítolo
Noble Compañía de Seguros

Los peligros vinculados a la tecnología de la salud pueden ser de muy distintos tipos. A veces son el resultado de problemas relacionados con la informática, tales como sistemas mal configurados, datos incompletos o inadecuada protección antivirus. Otros pueden ser originados por una mala interacción hombre-máquina, como ocurre cuando no se aplican técnicas correctas de reprocesamiento, no se mantienen los equipos o no se atienden a las advertencias de los fabricantes respecto de fallas identificadas. Los riesgos también pueden provenir de de problemas intrínsecos de los equipos: fallas de diseño, dificultad de uso, calidad defectuosa y fallas para desempeñarse como deberían. Todos estos factores pueden contribuir a la ocurrencia de eventos dañosos para los pacientes.

Resulta vital reconocer estos peligros y abordarlos antes de que causen problemas. Pero la gran pregunta es: ¿Por dónde comenzar?. Para ello, ECRI Institute, una de las Organizaciones de Seguridad del Paciente y de evaluación de tecnologías médicas más importantes del mundo elabora todos los años un listado con los 10 principales peligros de las tecnologías en uso en hospitales y centros de salud. Esta lista anual está diseñada para identificar potenciales fuentes de peligros que el Instituto considera que merecen especial atención en el próximo año. Busca ser una herramienta para que las instituciones prioricen sus esfuerzos en seguridad de los pacientes. La lista no cubre todos los peligros ni tampoco se aplica a todas las instituciones. Más bien, está diseñada como un punto de partida para las discusiones sobre seguridad de los pacientes y para establecer prioridades. Muchos de los peligros tampoco aplican a la mayoría de los hospitales y clínicas de la Argentina (ej: cirugía robótica). Sin embargo, se pueden extraer valiosas conclusiones cuando se abordan otros peligros (ej: reprocesamiento de endoscopios, confusión de vías IV, peligros de las alarmas, etc.)

---

* Traducción y adaptación del documento "Top 10 Health Technology Hazards for 2015. A Report from Health Devices. ECRI November 2014. Puede acceder al texto original en inglés ingresando al link: www.ecri.org/2015hazards

Los 10 peligros "top" para el 2015 son:

1. Alarmas: Riesgos por inadecuadas políticas y procedimientos de configuración

2. Integridad de los datos: Datos incorrectos o perdidos en las historias electrónicas y otros registros informáticos.

3. Confusión de vías intravenosas que lleva a una incorrecta administración de drogas y soluciones.

4. Inadecuado reprocesamiento de endoscopios e instrumental quirúrgico.

5. Desconexiones del respirador inadvertidas por alarmas mal configuradas o no atendidas.

6. Dispositivos de movilización de pacientes. Fallas del equipamiento y errores de los usuarios.

7. Acumulación de dosis radiactivas: Variaciones inadvertidas en la exposición a radiaciones diagnósticas.

8. Cirugía Robótica: Complicaciones por entrenamiento insuficiente

9. Seguridad cibernética: Insuficiente protección para sistemas y dispositivos médicos

10. Sobrecarga de recordatorios de fallas y alertas de seguridad para equipos electrónicos

1. Alarmas: Riesgos por inadecuadas políticas y procedimientos de configuración

Si bien muchos de los ejemplos de peligros vinculados a las alarmas que se brindan se relacionan con sistemas de monitoreo fisiológico, los conceptos que se discuten también aplican a otros dispositivos con alarma, como respiradores y bombas de infusión. La discusión sobre los temas de alarmas de desconexión de respiradores se discuten en detalle en el peligro Nº 5

Los médicos y enfermeras dependen de las alarmas de los dispositivos médicos para informarse rápidamente de cambios en la condición del paciente o de circunstancias que podrían afectar negativamente su atención. Cuando este sistema de advertencia falla o es inefectivo, los pacientes pueden sufrir daños serios, como lo evidencian numerosos reportes de lesiones graves y muertes asociadas a problemas con las alarmas.

Las estrategias para disminuir los peligros de las alarmas generalmente se focalizan en lo que se conoce como "fatiga de alarmas", una condición que puede llevar a no advertir las alarmas cuando el profesional se encuentra abrumado, distraído o desensibilizado por el gran número de alarmas que se activan. Sin embargo, la fatiga de alarmas no debería ser el único factor a considerar cuando las instituciones de salud trabajan para administrar mejor los sistemas de alarma clínica, tal como lo requiere el nuevo objetivo nacional de seguridad del paciente sobre seguridad de alarmas de la Joint Commission. En la experiencia de ECRI Institute, los eventos adversos vinculados a alarmas (que pueden involucrar tanto a alarmas inadvertidas como a condiciones no reconocidas de las mismas), suelen ser el resultado de prácticas inadecuadas de configuración.

Por eso, se estimula a las instituciones de salud a que examinen sus actuales normas y procedimientos de manejo de alarmas en sus esfuerzos por minimizar este riesgo, si es que todavía no lo han hecho.

Las prácticas de configuración de alarmas incluyen, por ejemplo, la determinación de qué alarmas deberían ser habilitadas, la selección de los límites a utilizar en cada alarma y el establecimiento del nivel de prioridad. Estas elecciones se basan típicamente en las necesidades particulares de cada área de atención y en la gravedad de los pacientes que se atienden en la misma, además de las condiciones fisiológicas de cada paciente específico.

Las prácticas inapropiadas de configuración de alarmas – es decir la selección de valores o configuraciones que no se corresponden con las circunstancias de atención del paciente, pueden llevar a que 1) los prestadores no se notifiquen cuando el paciente desarrolla una condición que debería gatillar la alarma. 2) los prestadores se encuentren expuestos a un excesivo número de alarmas, sobre todo de aquellas que suenan por condiciones clínicas insignificantes (ej: aquellas que no requieren una respuesta del personal)

Entre los algunos ejemplos de prácticas de configuración de alarmas inapropiadas se pueden incluir los siguientes:

- Falla para reconfigurar el dispositivo médico a los límites de alarma predeterminados cuando un nuevo paciente es conectado al dispositivo. En esta circunstancia, los niveles de alarma utilizados para el paciente previo serán utilizados para el nuevo paciente.

- Selección inapropiada de los límites de alarma para los parámetros que se monitorean (e; frecuencia cardíaca, saturación de oxígeno). Los rangos de límites muy amplios determinan que las alarmas no se activen hasta que la condición del paciente se ha deteriorado. Los límites muy estrechos, por otra parte, pueden llevar a excesivas activaciones, sobrecargando al personal con alarmas para condiciones que no son clínicamente significativas (llevando a la fatiga de alarmas).

- Selección de niveles de prioridad de alarma que no se corresponden con la seriedad de la condición y la velocidad de respuesta requerida. Una alarma para una condición que requiere atención inmediata, por ejemplo, no debería configurarse para activarse a una prioridad baja.

- No utilizar algunas alarmas de arritmias aún cuando el paciente tiene riesgo de experimentar una arritmia que puede requerir una intervención clínica

La configuración del volumen de las alarmas es otra práctica de configuración que debe revisarse. Las alarmas pasarán inadvertidas si se las setea a niveles inaudibles o si el sonido de la alarma es desactivado o silenciado indefinidamente, evitando que el personal actúe cuando se activa.

ECRI Institute ha investigado varias muertes relacionadas con alarmas y otros casos de lesiones severas que podrían haber sido prevenidas si hubieran existido o se hubieran seguido normas claras de configuración.

Recomendaciones

Primero, establecer una política describiendo prácticas de configuración de alarmas estándares para cada área específica. Si las normas ya existen, evaluar si las mismas son completas y clínicamente relevantes. La política de alarmas debería abordar factores tales como los siguientes:

- Parámetros predeterminados de alarmas (incluyendo límites y prioridades) que reflejen las necesidades e indicaciones clínicas y se adecuen al tipo de pacientes que se atienden en cada área.

- Configuración del volumen de las alarmas teniendo en cuenta las necesidades específicas de cada área.

- Proceso para modificar la configuración de la alarma- Por ej. quién está autorizado a realizar cambios, bajo qué circunstancias se pueden hacer y cómo serán documentados los mismos. La norma debería distinguir entre los cambios que pueden ser realizados por el personal de enfermería (ej: adaptar el límite de la alarma a la condición del paciente) y aquellos que requieren de un acceso más restringido (ej. para establecer los valores de default).

- Proceso para garantizar que las alarmas permanezcan con la configuración correcta durante y luego del traslado del paciente de un área o servicio a otra (ej: hacia y desde quirófanos).

- Proceso para reactivar los parámetros predeterminados para esa alarma cada vez que un nuevo paciente es conectado al dispositivo.

- Requisitos de entrenamiento para capacitar al personal clínico acerca de las normas de manejo de alarmas en la institución.

El personal médico y de enfermería debería tener un fácil acceso a la norma y de deberían auditar periódicamente los parámetros de configuración para garantizar el cumplimiento de la norma. Como las auditorías generales de cada área pueden ocupar mucho tiempo y recursos, puede pensarse en auditar muestras de monitores, chequeando las configuraciones más críticas.

2. Integridad de los datos: Datos incorrectos o perdidos en las historias electrónicas y otros registros informáticos

Hoy en día, muchas de las decisiones de atención se basan en los datos volcados en las historias clínicas electrónicas y otros sistemas informáticos. Cuando funcionan bien, estos sistemas brindan la información que los médicos y enfermeras necesitan para tomar decisiones de tratamiento correctas. Sin embargo, cuando hay fallas en el sistema o cuando se cometen errores, la información que termina apareciendo en la historia clínica puede ser incompleta, imprecisa o desactualizada, llevando a decisiones incorrectas con riesgo para los pacientes.

Lo que hace que este problema sea tan preocupante es que la integridad de los datos en los sistemas de registro computarizado puede comprometerse de muy diferentes maneras y, una vez introducido el error, el mismo puede ser muy difícil de identificar y corregir. Entre algunos ejemplos de fallas en la integridad de los datos se pueden incluir los siguientes:

- Aparición de los datos de un paciente en la historia clínica de otro (discordancia paciente/datos).
- Pérdida de datos o entrega retrasada de información (ej: por limitaciones de la red, errores de configuración o demoras en el ingreso de datos).
- Errores de configuración de fecha y hora entre distintos dispositivos y sistemas médicos.
- Valores por defecto (predeterminados) utilizados por error, o campos predeterminados con datos erróneos).
- Inconsistencias en la información sobre el paciente cuando coexisten las historias electrónicas con las de papel.

Los programas para reportar y analizar los problemas relacionados a la tecnología informática pueden ayudar a las organizaciones a identificar y rectificar las averías y fallas del sistema. Sin embargo, estos programas se enfrentan a desafíos importantes. El principal de ellos radica en que el personal de la primera línea de atención y los usuarios que reportan los eventos adversos (como así también el staff que los analiza) pueden no comprender exactamente el rol que el sistema informático jugó en el evento. Por ejemplo, sólo luego del análisis de un incidente en el cual el farmacéutico cargó la orden de medicación en la historia clínica equivocada se pudo reconocer que el error se vio facilitado por la posibilidad que tenía el sistema informático de administración de medicación que permitía que los usuarios tuvieran abiertas dos historias clínicas al mismo tiempo.

Recomendaciones

- Antes de implementar un nuevo sistema o de modificar el que existe, evalúe el flujo y tipo de trabajo de quienes serán los usuarios. Comprenda cómo será utilizado o está siendo utilizado el sistema por ellos. Identifique ineficiencias y potenciales fuentes de error.

|Por ejemplo, si los datos pasan directamente del dispositivo a la historia clínica electrónica, se debe prestar especial atención al proceso de asociación de la máquina al paciente, al corte del vínculo cuando el paciente es dado de alta o desconectado del aparato (disociación) y para que los profesionales verifiquen los datos antes de que sean guardados en la historia del paciente (validación).

- Pruebe cuidadosamente la historia electrónica o cualquier sistema de registro informático y sus interfases para verificar que el sistema se implementa de manera completa y que se comporta como se espera (durante la etapa de implementación inicial y luego de introducir cualquier cambio en el sistema). Asegúrese de incluir a la primera línea de atención en el análisis.
- Establezca un plan general de entrenamiento y haga que los usuarios demuestren competencia antes de estar autorizados a usar el sistema. Ofrezca a los usuarios una vía de ayuda rápida cuando se trabaja con un nuevo sistema o una nueva función.
- Establezca mecanismos para reportar e investigar todos los incidentes, eventos adversos y peligros relacionados con el uso de la tecnología informática. Utilice un equipo interdisciplinario (personal de sistemas, personal clínico, etc). en el proceso de análisis de incidentes.

3. Confusión de vías intravenosas que lleva a una incorrecta administración de drogas y soluciones

En listados previos de “los 10 principales peligros tecnológicos”, ECRI subrayó el papel que los errores de programación de las bombas de infusión tienen en los eventos adversos por mal manejo de la medicación. Este año, el foco no está puesto en la bomba, sino en la maraña de tubos que existen cuando se deben

administrar múltiples infusiones intravenosas a un solo paciente, una ocurrencia muy frecuente en la atención de todos los días.

Si una medicación o solución IV es administrada en un sitio de infusión incorrecto, o a una velocidad equivocada, las consecuencias pueden ser severas. Hay varias formas en los que esto puede pasar, por ejemplo:

- La vía de infusión puede estar conectada a una bolsa con una solución errónea. Esto determinará que se administre una medicación que no corresponde, o que la solución sea administrada a una velocidad errada o a través de una ruta equivocada.

- La vía de infusión puede estar instalada en una bomba o canal de infusión equivocado. Esto podría derivar en una medicación o soluci ón administrada a una velocidad mayor o menor que la indicada.

- El extremo del paciente de la vía de infusión podría estar conectada a otra ruta no IV de administración. En algunos incidentes reportados, por ejemplo, la solución que debía pasarse por vía intravenosa fue pasada por un catéter epidural.

No llama la atención que la posibilidad de errores aumente cuando hay muchas guías y sueros. Un estudio encontró que la probabilidad de ocurrencia de un evento adverso aumenta un 3% por cada medicación intravenosa adicional que se administra (Kane-Gill et al, 2012).

Dentro de los factores que contribuyen a la confusión con las vías de infusión se incluyen los siguientes:

- El número de líneas de infusión presentes. Algunos pacientes de terapia intensiva o de procedimientos quirúrgicos pueden llegar a tener más de 12 líneas al mismo tiempo. Además, cuando se monta una infusión sobre la misma línea que el paciente tiene puesta (“piggyback”), la línea de infusión primaria y la secundaria y sus dos bolsas pueden quedar asociadas a una sóla bomba o canal pudiendo haber errores en el volumen inyectado.

- La variedad de vías de administración de medicamentos. Si bien las bombas se utilizan mayormente para pasar medicamentos y soluciones por vía intravenosa, también pueden ser utilizadas para vías epidurales, subcutáneas o arteriales. De ahí el potencial de que una solución indicada para una vía sea administrada erróneamente por otra.

- Dificultad para distinguir visualmente una línea de la otra. La maraña de líneas de infusión hace que muchas veces sea difícil trazar la línea desde la bolsa con la solución hasta el paciente. Este problema aumenta cuando la línea se encuentra tapada por la bata del paciente o por sábanas.

- La incapacidad de las bombas de infusión para distinguir una línea de otra. No existe ningún método automático para asociar una bomba o canal de infusión con una solución o vía de administración específica.

Recomendaciones

Muchos investigadores y organizaciones han publicado recomendaciones para reducir los riesgos asociados con la confusión de líneas de infusión IV. Las letras entre paréntesis que figuran más abajo hacen referencia a la fuente para cada recomendación, las cuales se insertan a continuación:

Para todas las instancias en las cuales se necesitan múltiples líneas IV para un solo paciente:

- Siga físicamente cada línea de infusión desde la bolsa con la solución hasta la conexión de ingreso al paciente, verificando que el conector dirija la solución hacia el sitio correcto de administración. (A), (B)

- Etiquete cada línea de infusión con el nombre de la droga o solución que está siendo administrada. (C) ,(D), (E-F. Fase 2b)

- No fuerce ni adapte conectores. Si una conexión resulta dificultosa (si requiere mucho esfuerzo, tal vez no debería realizarla. (A)

Cuando se compran suministro y equipamiento:

- Utilice productos con estándares de calidad aprobados por el regulador (en la Argentina ANMAT). No compre adaptadores que permitan conexiones erróneas.

- Considere adicionar broches, lazos o velcro en los hombros y mangas de las batas de los pacientes para facilitar el seguimiento de la línea y los cambios de bata. (E/F-Fase 1b, Fases 2a y 2b)

Para infusiones epidurales en particular, deberían considerarse los siguientes abordajes:

- Utilice líneas de color amarillo sin puertos de inyección (G)

- Coloque la bomba de infusión epidural en el sitio opuesto a la bomba que se utiliza para la infusión IV (G)

- Utilice para las infusiones epidurales un modelo de bomba diferente al que utiliza para infusiones IV (G)

Fuente de estas recomendaciones:

(A) ECRI Institute
(B) Cassano-Piché et. al (Ver Ontario Health Technology Assesment Series, Fase 1b)
(C) Pennsylvnia Patient Saferty Authority (Ver: Wollitz and Grissinger)
(D) The Joint Commission
(E) HumanEra (antes the Haelth Technology Safety Research Team; ver Ontario Health Technology Assessment Series.
(F) Institute for Safe Medication Practices Canada (ISMP Canada; ver Ontario Health Technology Assessment Series)
(G) Institute for Safe Medication Practices.

4. Inadecuado reprocesamiento de endoscopios e instrumental quirúrgico

Mientras ECRI preparaba la lista de riesgos tecnológicos 2015, el virus del Ébola pasó a ocupar la primera plana de los diarios de todo el mundo. La naturaleza altamente contagiosa de esta enfermedad subraya la importancia crítica de la función de reprocesamiento (limpieza y desinfección o esterilización de objetos que pueden contaminarse durante su utilización con un paciente) Los procedimientos de reprocesamiento inadecuados ponen en riesgo a los nuevos pacientes que entran en contacto con estos equipos.

Cada día, las instituciones de salud reprocesan miles de dispositivos e instrumental quirúrgico no descartable para ser utilizado en nuevos procedimientos. Cuando se realiza adecuadamente, el reprocesamiento remueve los residuos y los materiales potencialmente infecciosos, desinfectando o esterilizando el instrumental para que pueda ser reutilizado con seguridad en el próximo paciente. Cuando no se hace bien, en cambio, los patógenos pueden diseminarse a los nuevos pacientes, llevando a infecciones hospitalarias y eventuales brotes de la enfermedad.

Si bien la incidencia de las fallas de reprocesamiento es muy baja, sus consecuencias pueden ser muy graves. De las 13 amenazas inmediatas de vida reveladas en encuestas realizadas por la Joint Commission en 2013, siete estaban relacionadas directamente con la inadecuada esterilización o desinfección de equipos que requerían altos niveles de desinfección. (Joint Commission. I high level disinfected equipment –online- Quick Safety 2014 May.). Este tema, que ya figuró en la lista de "los 10 riesgos principales" de otros años, continúa estando entre las prioridades porque a través de los medios y de reportes se siguen viendo casos de daños por utilización de instrumental potencialmente contaminado.

Un paso crítico del reprocesamiento, pero que generalmente es pasado por alto o es realizado de manera inconsistente, es la limpieza inicial del dispositivo o instrumental en el sitio de uso (ej: sala de procedimientos, quirófano). Si los restos orgánicos y otros contaminantes no son removidos adecuadamente en este primer paso, la desinfección o esterilización

efectiva del dispositivo o instrumental puede no ser posible. Utilizando los endoscopios flexibles como ejemplo, los detritus que no son removidos tanto de la superficie exterior como del interior los canales del endoscopio durante una primera fase de lavado, pueden luego secarse y formar una placa impenetrable, o las bacterias existentes pueden formar un biofilm. Cualquiera de estas dos situaciones puede hacer fracasar a los agentes germicidas utilizados para desinfectar o esterilizar las superficies que se encuentran por debajo de estas capas.

El reprocesamiento de endoscopios es particularmente difícil porque estos dispositivos tienen canales de luz muy estrecha difíciles de limpiar. Más aún, e proceso involucra muchos pasos (generalmente específicos para cada modelo) que necesitan ser seguidos con gran diligencia para garantizar que el dispositivo se encuentra en condiciones para el próximo paciente. Casi todos los años, distintas instituciones de salud le piden a ECRI que investigue sus fallas en el reprocesamiento de endoscopios para ayudarlos a establecer un proceso más efectivo.

Entre los factores que pueden llevar a una limpieza inadecuada del instrumental se incluyen la complejidad del mismo (ej: dispositivos con canales muy estrechos o con partes removibles), instrucciones de limpieza del fabricante muy largas o incompletas, presiones de tiempo sobre el personal que limpia y desinfecta los equipos y falta de entrenamiento del personal, por sólo nombrar algunos.

Recomendaciones

- Enfatice con el personal de reprocesamiento y con los usuarios finales la importancia de una limpieza profunda de los dispositivos e instrumental antes de la desinfección o esterilización.

- Brinde el espacio, el equipo y los recursos necesarios para que la función de reprocesamiento pueda ser realizada de manera efectiva. Debería disponerse de un espacio tal que permita que el equipo pueda ser reprocesado y guardado fuera de áreas con intenso tráfico de personal. La mesada de trabajo debería contar con la superficie suficiente como para que los instrumentos sucios y limpios estén lo suficientemente separados para evitar contaminación cruzada. Además, las áreas de procedimientos deberían contar con el instrumental suficiente como para satisfacer la demanda, y debería destinarse el tiempo necesario a la tarea de limpieza y desinfección. La falta de endoscopios e instrumental en la cantidad necesaria, sumado al poco tiempo otorgado a quienes los limpian y desinfectan para tenerlos nuevamente disponibles para procedimientos electivos, podría crear un ambiente en el cual el personal estaría tentado a tomar atajos peligrosos (ej: salteándose pasos en el procedimiento de reprocesamiento.

- Garantice condiciones ambientales apropiadas para la tarea, como una adecuada filtración de agua y temperatura de agua de limpieza aceptable.

- Confirme la existencia de un adecuado protocolo de reprocesamiento, y que el mismo se encuentre rápidamente disponible para todos los modelos de endoscopios e instrumentos relevantes, incluyendo los de su propio inventario y los de cualquier dispositivo alquilado que podría ser utilizado. Refiérase a los manuales de usuario y consulte a los fabricantes para identificar requisitos específicos que deben abordarse. (ej: procedimientos de limpieza, adaptadores para canales)

- Verifique que estos protocolos aborden y documenten todos los pasos del reprocesamiento con el suficiente nivel de detalle (desde el pre-lavado en el sitio de uso -cuando es apropiado-, hasta el transporte seguro y aséptico del equipo hacia el sitio de depósito hasta su próximo uso.)

- Brinde un adecuado entrenamiento en lavado y reprocesamiento del instrumental apenas el personal que estará involucrado en el proceso se une a su organización. También cuando se utilizarán nuevos instrumentos o se modificarán los procesos del servicio al respecto. Repita la capacitación periódicamente para mantener la competencia.

- Revise periódicamente los protocolos para garantizar que los mismos sean claros, completos, precisos y actualizados, por ejemplo, reflejando los flujogramas vigentes de trabajo y el instrumental y los químicos en uso. Tenga en marcha mecanismos para garantizar que los procedimientos están actualizados y que se notifique al personal cuando los proveedores de equipos y dispositivos actualizan sus instrucciones de reprocesamiento.

- Monitoree la adherencia a los protocolos de lavado del instrumental.

- Recabe la opinión del personal que limpia y desinfecta los instrumentos antes de comprar nuevo equipamiento para identificar dispositivos que requieran de tiempo adicional o nuevos pasos para reprocesarlos efectivamente. Estos factores pueden influir en las decisiones de compra.

- Favorezca la comunicación y colaboración entre el personal de reprocesamiento y los servicios a los que éstos apoyan.

5. Desconexiones del respirador inadvertidas por alarmas mal configuradas o no atendidas

Los respiradores son dispositivos de soporte vital que suministran presión positiva a pacientes que requieren asistencia total o parcial para mantener una adecuada ventilación. Una desconexión completa o parcial en cualquier punto del circuito que transporta los gases entre el respirador y el paciente puede rápidamente llevar a este último a la anoxia cerebral con daños irreversibles y eventualmente la muerte.

Para prevenir esta ocurrencia, los respiradores incorporan sensores y alarmas para advertir a los prestadores cuando ocurre una desconexión, ya sea esta una completa separación de un componente del circuito respiratorio o una desconexión parcial que permita la fuga de gases del sistema. Sin embargo, para que estas alarmas sean efectivas, deben estar configuradas adecuadamente y deben poder ser oídas cuando suenan. ECRI Institute ha investigado casos en los cuales los pacientes sufrieron daños serios por alarmas configuradas en niveles inapropiados o porque el personal no escuchó las alarmas cuando éstas se activaron.

Estas alarmas son críticamente importantes no sólo por las consecuencias severas que puede tener una desconexión sino también porque la incidencia de desconexiones es relativamente alta.. Las tubuladuras generalmente incorporan varias secciones de tubos y una variedad de otros componentes como humidificadores o nebulizadores. Estos componentes se encuentran conectados por ensambles de fricción, sin que existan mecanismos de cierre. Por lo tanto, la conexión insegura de los componentes al ensamblar los circuitos o el movimiento intencional o no de los componentes del mismo durante su uso (por el personal, por el paciente o por la familia), pueden hacer que estos componentes 1) se aflojen en cualquiera de los puntos de conexión, resultando en fugas o 2) se desconecten totalmente uno del otro. Cualquiera de las dos situaciones impide la adecuada ventilación del paciente. Además de los reportes de desconexiones a nivel de las tubuladuras del respirador, ECRI, como Patient Safety Organization ha recibido reportes de auto-extubaciones, en las cuales el propio paciente removió su tubo endotraqueal. Las recomendaciones brindadas aquí acerca de la configuración y audibilidad de las armas también aplican para estos casos.

Muchos modelos de respiradores tienen incorporada una alarma automática específica para desconexiones del circuito; la misma no puede ser configurada por el usuario. Si bien esta alarma brinda cierta protección, no debería dependerse exclusiva mente de ella para advertir una desconexión. Son varios los factores que pueden afectar la activación de esta alarma, incluyendo la configuración del respirador que se está utilizando en ese momento, las condiciones que aparecen como resultado de la desconexión (ej: resistencia al flujo en el sitio de desconexión), y cómo ha sido diseñado el respirador para responder a tales condiciones.

Una forma más confiable para detectar desconexiones consiste en verificar que las alarmas programables por los usuarios se encuentren adecuadamente configuradas, en particular las de baja presión y las de bajo volumen minuto. Una desconexión parcial o completa del circuito respiratorio provocará un

descenso en la presión del mismo, activando la alarma de presión baja (si se encuentra configurada adecuadamente). A esto se suma que la desconexión provocará un descenso en el volumen de gas que retorna al respirador, condición que debería activar la alarma de bajo volumen minuto.

Sin embargo, si la configuración de estas alarmas no es elegida cuidadosamente, aquellas circunstancias que resultan en sólo una pequeña caída en la presión del circuito o en un descenso gradual y no abrupto de los volúmenes de retorno luego de una desconexión podrían no activar las alarmas. Entre los ejemplos se pueden incluir aquellas instancias en las cuales la parte terminal del circuito desconectado se encuentra ocluida (por ejemplo por las propias sábanas del paciente) y los casos en los cuales el circuito respiratorio incluye componentes que generan una alta resistencia (ej: cánula de traqueostomía de pequeño calibre)

ECRI Institute ha investigado incidentes en los cuales la alarma de baja presión estaba programada a un nivel significativamente más bajo que la presión del pico inspiratorio del paciente. En niveles de ajuste muy bajos, la alarma queda desactivada funcionalmente, requiriendo un gran descenso en la presión y ventilación para activarse. Similarmente, se han observado casos en los cuales los clínicos configuraron la alarma de bajo volumen minuto a niveles tales que sólo se activaban cuando el paciente recibía muy poco oxígeno como para mantener la vida.

Adicionalmente, aún aquellas alarmas bien configuradas serán inefectivas si no son escuchadas por las enfermeras y médicos. Entre los factores que pueden impedir que las alarmas sean escuchadas se incluyen a las puertas de las habitaciones cerradas total o parcialmente, pasillos largos, ruido ambiental y ajustes del volumen de las alarmas a niveles bajos que no tienen en cuenta la distancia entre el prestador y el respirador.

Algunas instituciones utilizan sistemas de notificación de alarmas auxiliares como una forma de anunciar alarmas de manera remota fuera de la habitación del paciente. Si se utilizan estos sistemas, la institución debe verificar que todas las alarmas relevantes y la información sobre las mismas (ej: nivel de prioridad) sea comunicado efectivamente al personal.

Recomendaciones

- Desarrolle y documente una norma para configurar las alarmas de baja presión y de bajo volumen minuto del respirador a niveles que sean apropiados para detectar desconexiones. Un alarma de baja presión está bien programada cuando se activa entre 5 a 7 cm H2O por debajo de la presión del pico inspiratorio del paciente. La alarma de bajo volumen minuto no debería configurarse más allá del 15% por debajo del volumen minuto requerido por el paciente. Las instituciones pueden personalizar estos valores, ajustándolos a lo que resulta apropiado para cada paciente. Los médicos y enfermeras involucradas con respiradores deberían conocer esta norma y el rol que juegan las alarmas de baja presión y volumen minuto en la detección de desconexiones.

- Instruya a todo el personal clínico para que confirme que aquellas alarmas de baja presión y bajo volumen minuto que funcionan de otra manera se encuentran dentro del rango correcto (Ej: configuraciones predeterminadas, configuraciones que utilizan el “autoset” disponible en algunos respiradores, etc.)

- Solicite a los terapistas que confirmen, durante sus chequeos regulares del respirador, que todas las alarmas se encuentran activas y adecuadamente programadas y que examinen la totalidad del circuito para verificar que todas las conexiones se encuentran seguras

- Solicite a las enfermeras que revisen el sistema para verificar que todas las conexiones del circuito se encuentran seguras luego de mover al paciente (reposicionamiento del paciente, regreso a la unidad luego de traslados, etc.)

- Determine si las alarmas pueden ser adecuadamente oídas en las áreas en las que se utilizará el respirador. Asegúrese de considerar cualquier barrera potencial que pudiera aparecer en el ambiente (puertas cerradas, excesivo ruido, etc.)

- Si se utilizan sistemas auxiliares de notificación de alarmas para ser utilizados para controlar remotamente las desconexiones: Establezca claramente las necesidades técnicas y clínicas y las expectativas para la notificación del sistema; pruébelo a conciencia antes de comprarlo y cuando se realizan cambios en el software, ya sea del respirador o del sistema auxiliar de notificación. Evalué la forma en la que cada alarma será comunicada al personal clínico mediante este sistema auxiliar, considerando el tipo de información que será comunicada (tipo de alarma, nivel de prioridad). Examine también si existen alarmas para advertir interrupciones en la comunicación entre el respirador y el sistema de control remoto (ejemplo por desenchufarse algún cable); Se deberá entrenar al personal en la identificación de circunstancias que pueden causar estas disrupciones.

.

6. Dispositivos de movilización de pacientes. Fallas del equipamiento y errores de los usuarios

Los hospitales se encuentran entre los lugares más peligrosos para trabajar en los Estados Unidos, de acuerdo a un informe de la Administración de Seguridad y Salud Ocupacional (OSHA). Y las lesiones del personal vinculadas con el levantamiento, transferencia o movilización de pacientes son una de las principales razones para que así sea. Una investigación de esta oficina gubernamental reportó, luego de realizar una encuesta a cerca de 1.000 hospitales, que las lesiones vinculadas a la movilización de los pacientes representaron el 25% de todos los reclamos del sector salud ante las administradoras de riesgos del trabajo en 2011. Por otra parte, los pacientes también pueden ser dañados si estas actividades no son llevadas a cabo efectivamente.

Existe una gran variedad de dispositivos y tecnologías disponibles para ayudar a reducir el riesgo del personal y de los pacientes durante este tipo de actividad. Entre los ejemplos se incluyen una gran variedad de diseños para elevar y transferir pacientes que van desde equipos especiales de elevación de pacientes obesos (Grúas montadas en el techo o móviles, modelos que ayudan a pasar de la posición sentada a la parada), ayudas de transferencia lateral (tablas, deslizadores, material rodante, colchones inflables, junto con sillas y camillas especiales. sin embargo, el uso inapropiado de estos dispositivos, su falta de mantenimiento o fallas intrínsecas de los mismos pueden llevar a lesiones.

Los reportes de incidentes con estos equipos notificados a la FDA y otras fuentes describen cómo la mala utilización de esta tecnología puede llevar a lesiones, por ejemplo:

- **Uso inapropiado de elevadores de pacientes (distintos diseños).** Ej: Un cabestrillo que no está sujeto adecuadamente, una sobrecarga de peso para el elevador o la utilización de un elevador para transportar al paciente cuando no estaba diseñado para ese propósito.

- **Problemas asociados con elevadores móviles.** Las pruebas realizadas por ECRI sobre elevadores portátiles de pacientes encontraron que algunos de estos dispositivos pueden deformarse cuando se sobrecargan. Además, la FDA observó que la inclinación del elevador también es un problema, por ejemplo si el peso del paciente se desplaza o si el elevador no está posicionado correctamente debajo de la cama.

- **Problemas asociados al uso de tablas de transferencia.** Cuando se utilizan estos dispositivos (que son tablas rígidas que facilitan el deslizamiento del paciente de una superficie a otra, se debe tener especial cuidado para evitar fricciones, cuando se inserta la tabla debajo del paciente, particularmente en aquellos que tienen quemaduras o úlceras por decúbito.

También es importante que los equipos de transferencia sean inspeccionados y mantenidos adecuadamente. Para prevenir o para identificar y rectificar problemas que pueden llevar a lesiones. Los equipos dañados, rotos o defectuosos, que no han sido limpiados o con baterías que no han sido adecuadamente cargadas no estarán disponibles para usarlos cuando se necesiten o bien expondrán al paciente/personal a sufrir lesiones.

Las fallas intrínsecas de los dispositivos también son un problema. Distintas alertas de seguridad publicadas por

ECRI Institute documentan la variedad de fallas que pueden aparecer , tanto durante el uso normal del equipo como por una mala utilización o errores en la manufactura o diseño del mismo (desprendimientos de la grúa del techo, fracturas de los brazos u otros componentes del elevador, problemas con el deslizador, problemas eléctricos, etc.

Recomendaciones

Primero, capacitar a los prestadores para reconocer escenarios que pueden llegar a requerir el uso de equipamiento especial para movilizar pacientes. De acuerdo a un reporte del Instituto Nacional de Seguridad y Salud Ocupacional, el límite máximo de peso recomendado para la mayoría de las tareas de movilización de pacientes bajo condiciones ideales (ej: pacientes no agresivos) es de 35 lb -16 kilos- (Waters et al, 2009). Por lo tanto, tratar de levantar, mover o transferir aún a pacientes livianos puede ser peligroso. De particular preocupación son aquellas actividades que colocan al prestador en posiciones incómodas o que requieren levantar mucho peso, por ejemplo:

- Transferir a pacientes del inodoro a una silla, de una silla a la cama o de la bañadera a una silla.
- Reposicionar a un paciente de lado en una cama o silla.
- Levantar a un paciente de la cama.
- Extender la cama con el paciente acostado.
- Lavar al paciente en la cama.
- Ayudar al paciente a movilizarse y deambular.
- Vestir al paciente.

Segundo, facilitar el adecuado uso de los dispositivos para levantar y movilizar pacientes con el objetivo de minimizar el riesgo de lesiones del personal o de los pacientes. Para hacer esto:

- Capacite al personal acerca de la necesidad de estos dispositivos, y entrénelo para que los manejen adecuadamente.
- Provea suficientes equipos de manera tal que los mismos se encuentren rápidamente disponibles cuando se necesiten, y almacene los dispositivos y accesorios en lugares de fácil acceso.
- Seleccione equipos con límites de carga que se correspondan con el tipo de población que se atiende. Capacite además al personal acerca de los límites de peso para cada pieza de equipamiento y de los riesgos de exceder ese límite.
- Instituya un programa para manejar los accesorios (ej: cargadores de baterías de los elevadores, almacenamiento de bretes y soportes de manera organizada en localizaciones convenientes.

Tercero, establecer responsabilidades para la inspección oportuna, el mantenimiento preventivo y la reparación de los equipos de movilización de pacientes y accesorios (ej; bretes), y cumplir con las guías apropiadas para estas actividades.

7. Acumulación de dosis radiactivas: Variaciones inadvertidas en la exposición a radiaciones diagnósticas

La acumulación de dosis (“Dose Creep”) es un patrón de exposición a niveles de radiación (ej: dosis) aumentados de a poco y a lo largo del tiempo por los técnicos y médicos en la búsqueda de imágenes de mejor calidad en radiología diagnóstica. Si bien es poco probable que esto derive en daños inmediatos, se trata de un problema insidioso que puede tener consecuencias a largo plazo y que, a través del tiempo, puede terminar afectando a muchos pacientes. Afortunadamente, comienzan a estar disponibles en la actualidad herramientas para ayudar a las instituciones de salud a combatir este peligro.

De alguna manera, la acumulación de dosis radiactivas (“dose creep”) es una consecuencia no deseada del progreso desde la radiología diagnóstica convencional a la digital.

Con cualquier tecnología de imágenes que utiliza radiaciones ionizantes, la exposición a dosis mayores se asocia con mayores riesgos para los pacientes (ej: aumento en la posibilidad de desarrollar cáncer a largo plazo). Por eso, los estándares de práctica especifican que los técnicos deben utilizar la dosis mínima indispensable para poder llegar a la información diagnóstica que se necesita. En otras palabras, la dosis de radiación no debería ser mayor ni menor de lo que se necesita para obtener una imagen de calidad.

En la radiología convencional, la exposición del paciente a niveles de radiación muy altos o muy bajos tienen una penalidad: las imágenes aparecen muy penetradas o muy blandas, impidiendo su uso. Por lo tanto, los desvíos muy amplios de la exposición óptima son fácilmente advertidos.

La radiología digital, en cambio, es más condescendiente. Como se maneja con un rango de dosis dinámico y más amplio que el de la radiología convencional, puede tolerar parámetros de exposición significativamente más altos o bajos y obtener aún así imágenes de buena calidad. Una de las ventajas de este rango mayor es que reduce la posibilidad de que una imagen deba ser repetida, no sobreexponiendo al paciente a más radiación si la dosis utilizada fue mayor o menor a la necesaria.

Una desventaja de la radiología digital, sin embargo, es que este rango dinámico más amplio genera un ambiente en el cual los técnicos radiólogos pueden ajustar los parámetros de exposición por fuera de los niveles recomendados, realizando a veces pequeños cambios a lo largo del tiempo, sin que exista una indicación obvia para estos cambios. Por lo tanto el desvío de la exposición recomendada no es por lo general evidente al observar la imagen digital resultante.

De hecho, en la radiología digital la calidad de la imagen generalmente mejora cuanto mayor es la dosis de radiación. Por ello, existe la tendencia natural a ajustar la dosis en niveles altos para obtener una mejor imagen. Estos pequeños ajustes repetidos a lo largo del tiempo pueden llevar a la utilización de factores de exposición que varían sustancialmente de la exposición “usual” recomendada para un determinado estudio, sin que los usuarios adviertan que los niveles de dosis han sido aumentados.

La consecuencia es que los pacientes pueden quedar de rutina expuestos durante sus exámenes a dosis de radiaciones ionizantes innecesariamente altas. Si bien los efectos de cualquier aumento de dosis en un solo estudio son despreciables, el efecto acumulativo sobre pacientes sometidos a múltiples estudios durante el curso de su tratamiento puede ser significativo, particularmente en neonatos.

Con las imágenes digitales, la única forma objetiva de identificar si los factores de exposición óptima son utilizados consistentemente (ej: para todos los estudios en todas las áreas de atención), consiste en revisar los indicadores de exposición provistos por cada equipo de imágenes. Anteriormente, la práctica de comparar los indicadores de exposición en los distintos equipos o áreas de atención resultaba complicada por la falta de un abordaje estandarizado. Cada fabricante definía sus propios indicadores numéricos de exposición radiológica para estimar la dosis disparada. Últimamente, sin embargo, los fabricantes adoptan cada vez más el Índice de Exposición Estandarizado (Standarized Exposure Index –IE-) establecido por la International Electrotechnical Commission (IEC Standard 62494-1). Esto significa que las instituciones de salud pueden comenzar a utilizar el EI (en sistemas equipados debidamente) para auditar los factores de exposición que se utilizan y para identificar tendencias que indiquen variaciones con respecto a los valores óptimos.

Los nuevos equipos de imágenes comienzan a incorporar este estándar EI. También es posible, mediante una actualización del software, agregar esta capacidad en los equipos de radiología digital existentes. A esto se agregan nuevas herramientas de software que facilitan el seguimiento de los valores Para hacer un uso efectivo del Estándar EI, los jefes de radiología, posiblemente en consulta con los físicos, necesitarán definir valores aceptables para estudios específicos y tipos de pacientes, siguiendo la variación y encontrando formas para identificar prácticas deficientes.

Recomendaciones

- Si sus sistemas de radiología digital no están todavía equipados para utilizar el Índice de Exposicion Estandarizado (IE) desarrollado por

la International Electrotechnical Commission (IEC 62494-1) y la American Association of Physicists in Medicine (AAPM TG-116) e implementado por los fabricantes, investigue si es posible actualizar el software para añadir esta capacidad. Para la adquisición de nuevos equipos, solicite que tengan incorporada esta función.

- Luego de incorporar el estándar EI en sus sistemas de imágenes, utilícelo para estimar la dosis y exposición del paciente en el detector.

- Adopte los pasos que sean necesarios para mostrar los valores EI a los técnicos radiólogos como parte de su trabajo de rutina. Esto puede llegar a requerir una actualización del software o cambios en su configuración.

- Instale herramientas de software que automáticamente importen y analicen los datos de exposición (EI)

- Defina responsabilidades para auditar y analizar los datos EI en todo el departamento.

- Trabaje para definir valores y rangos EI aceptables para los estudios radiológicos más comunes.

8. Cirugía Robótica: Complicaciones por entrenamiento insuficiente

Los sistemas de cirugía robótica son dispositivos complejos que modifican el proceso quirúrgico para todos los involucrados. Como con cualquier nueva tecnología que obliga a abandonar una forma de abordaje previa, la preparación y el entrenamiento de los usuarios es fundamental para una cirugía segura. Si los cirujanos, el resto del equipo quirúrgico y el personal auxiliar no están lo suficientemente entrenados en el manejo del sistema robótico y en cómo operar bajo estas condiciones únicas, los pacientes pueden sufrir daños.

De hecho, ECRI Institute ha investigado varios eventos adversos vinculados específicamente a la cirugía robótica. Los eventos ocurrieron por factores tales como:

- La necesidad de reposicionar a los miembros del equipo o al instrumental para acomodarse al tamaño del robot.

- El reposicionamiento del paciente o movimientos accidentales de la mesa de cirugía durante el procedimiento.

- Lapsus en prácticas habituales de seguridad y comunicación del equipo, que llevan a complicaciones evitables. (ej: quemaduras por plancha del electrobisturí, oblitos, perforación de víscera hueca, etc.)

Por lo tanto, para minimizar riesgos a los pacientes, resulta esencial que las instituciones equipadas con estos sistemas garanticen el adecuado entrenamiento, acreditación y evaluación continua de la competencia requerida.

Actualmente, existe en el mercado sólo una línea de sistema robótico multipropósito: El Sistema de Cirugía Intuitiva da Vinci. Todos los sistemas da Vinci incluyen un carro que incorpora brazos robóticos equipados con instrumentos quirúrgicos y dispositivos endoscópicos especialmente diseñados. Este carro es posicionado cerca del paciente durante la cirugía. El equipamiento accesorio, como el equipo de video, la fuente de luz del endoscopio y la unidad de electrocauterio es colocado en un segundo carro adicional. Durante la cirugía, el cirujano (ubicado sobre una consola de control a varios pies del paciente y del resto del equipo quirúrgico) manipula los controles con sus manos y pies para posicionar y operar los brazos robóticos mientras mira las imágenes en tiempo real en un video 3 -D.

La habilidad y competencia del cirujano para utilizar un sistema tan complejo es un factor mayor para determinar si el sistema robótico puede ser utilizado con seguridad. Primero, el cirujano debe dominar los controles de la cámara, los movimientos de los brazos robóticos, la manipulación del instrumental y la activación de los dispositivos accesorios (ej: electrrobisturí). Una vez establecida su competencia en estas operaciones básicas, el cirujano debe adquirir e incorporar las técnicas de cirugía robótica específicas del procedimiento a realizar. Por último, deberá tener la

capacidad de responder adecuadamente ante circunstancias imprevistas, como movimientos accidentales de los brazos robóticos que hacen, por ejemplo, que los instrumentos queden atorados enganchados entre sí, a veces fuera de su campo visual.

Y no se trata sólo de la habilidad del cirujano, sino también del entrenamiento de todo el equipo de quirófano. La utilización de un robot altera las circunstancias de la cirugía para todos los involucrados. Por lo tanto, todo el personal, desde quien ayuda a posicionar al paciente pasando por circulantes, instrumentadoras y anestesiólogos deben ser especialmente entrenados para desarrollar las funciones que se requieren durante los procedimientos robóticos.

Recomendaciones

Las circunstancias de la cirugía asistida por robots obligan a adoptar un abordaje "robot-céntrico" a la hora de pensar cómo se entrenará a los cirujanos y al resto del equipo, de cómo se evaluará su competencia y de cómo serán realizadas ls actividades asociadas (desde la toma de decisiones hasta como limpiar el equipo luego del procedimiento). La revisión de todos los factores a considerar exceden los objetivos de este artículo. Aquí el foco está puesto en el rol del entrenamiento y la acreditación en la protección de los pacientes.

Si bien distintas sociedades científicas, organizaciones de cirugía robótica, aseguradores y agencias gubernamentales han desarrollado guías de práctica, no existe un consenso estándar que especifique la manera de entrenar y acreditar a los cirujanos y al personal para realizar procedimientos robóticos. Los hospitales deberán tomar sus propias decisiones, utilizando los recursos mencionados como guía.

Los factores a considerar cuando se desarrollan o evalúan los planes de entrenamiento y acreditación incluyen lo siguiente:

- **Entrenamiento del cirujano**; El entrenamiento debe abordar, entre otras cosas:

  - Las capacidades y limitaciones de la tecnología
  - Abordajes de cirugía robótica, como la colocación óptima de puertos y pasos del procedimiento
  - Estrategias para reducir el riesgo de producir lesiones (o dejar objetos) fuera del campo visual.
  - Resolución de problemas y técnicas de respuesta para manejar complicaciones durante el procedimiento.

Un programa de entrenamiento quirúrgico completo probablemente requerirá que el cirujano cumpla con una determinada cantidad de procedimientos robóticos, haya participado como ayudante previamente, pueda demostrar entrenamiento en simuladores, y haber operado bajo la supervisión de un tutor.

- **Entrenamiento de enfermería.** Las enfermeras e instrumentadoras también requieren de un entrenamiento especializado para estar a tono con las mayores demandas de los procedimientos robóticos. La capacitación debería cubrir:

  - Adecuada colocación de campos
  - La forma de asegurar la posición de la mesa de operaciones y los protocolos para realizar cambios de posición de la mesa durante el procedimientos
  - La adecuada colocación e interconexión de los dispositivos accesorios, tales como la unidad del electrobisturí y electrodos.

- **Entrenamiento del equipo**. Durante las cirugías robóticas debe existir una comunicación efectiva y colaboración entre el cirujano, sus cirujanos ayudantes, el anestesiólogo, la instrumentadora y resto del personal auxiliar. Por lo tanto, además del entrenamiento individual debe haber el suficiente entrenamiento en trabajo en equipo.

- **Entrenamiento del personal auxiliar**. El personal de esterilización, por ejemplo, deberá estar entrenado en los diferentes procedimientos de esterilización para cada parte del sistema robótico.

- **Acreditación**. Las decisiones de acreditación deberían basarse en la demostración de

competencia, la cual debería ser evaluada por cirujanos expertos en cirugía robótica; estas decisiones no deberían dejarse en manos de la industria. Si bien la realización de un número predeterminado de casos puede ser utilizada como guía, la casuística no debería reemplazar a la demostración de competencia. De manera similar, el entrenamiento en simuladores, si bien puede ser una herramienta efectiva, no debería tomar el lugar de cirugías realizadas con un tutor.

- **Mantenimiento de la competencia.** Además del entrenamiento inicial, los cirujanos y el resto del equipo necesitan utilizar frecuentemente el sistema robótico para no perder sus habilidades. Si la casuística para un procedimiento en particular es insuficiente para cumplir este requisito, considere si el entrenamiento en simuladores alcanzaría para mantener las habilidades necesarias. Tenga en cuenta que la necesidad de mantener el entrenamiento del personal – o de justificar el gasto- nunca debería ser un factor en la decisión de realizar una cirugía robóticamente.

Si bien la cirugía robótica se ha transformado en una alternativa válida para algunos procedimientos, todavía se trata de una tecnología en desarrollo, y sus aplicaciones probablemente se expandan en los próximos años. Por los tanto los criterios de acreditación y entrenamiento necesitarán ser rigurosamente evaluados y ajustados para acompañar los avances en la aplicación de esta tecnología.

9. Seguridad cibernética: Insuficiente protección para sistemas y dispositivos médicos

La creciente tendencia hacia la interconectividad y el trabajo en redes de los dispositivos médicos se asocia con un aumento en la vulnerabilidad de estos equipos a virus informáticos y a ataques maliciosos. Más allá de que hasta la fecha existen pocas evidencias de que estas vulnerabilidades produzcan un daño directo a los pacientes, la seguridad cibernética es un tema a considerar cuando se piensa en la seguridad de los pacientes y requerirá cada vez mayor atención en los próximos años.

Como lo observó la FDA, las protecciones de seguridad electrónica buscan prevenir la aparición de vulnerabilidades en los sistemas que puedan llevar a un mal funcionamiento de los equipos, a la interrupción de los servicios, al inapropiado acceso a la información de los pacientes o al compromiso de la integridad de los datos en las historias clínicas electrónicas.

Eventos como los siguientes ilustran la necesidad de estas protecciones:

- Un hospital tuvo que cerrar temporariamente su servicio de hemodinamia porque sus equipos se infectaron con un virus informático.

- Varias organizaciones de salud tuvieron que informar a sus pacientes y a la comunidad en general la pérdida, liberación o incluso el robo de información de salud protegida. Brechas de este tipo comprometen la seguridad y privacidad de los datos personales y pueden generar multas importantes y una publicidad muy negativa para la organización.

- Unos pocos investigadores han identificado vulnerabilidades específicas en algunos equipos médicos, manifestando su preocupación por su vulnerabilidad a “hackeos” y ataques maliciosos, lo que pondría en riesgo la seguridad de los pacientes. ECRI institute no ha sido notificado de ninguna circunstancia de daño a pacientes a consecuencia de hackeo de los dispositivos. Por ello, si bien el riesgo teórico amerita cierta observación, el riesgo real para la seguridad de los pacientes a partir de accionar de hackers mal intencionados parece ser mínimo, considerando los procesos de trabajo y las medidas de protección que típicamente se aplican en la práctica médica.

La protección de los equipos médicos contra virus informáticos que pudieran afectar su funcionalidad o la integridad de los datos de los pacientes es una medida clave de seguridad electrónica. Desafortunadamente, las instituciones de salud se enfrentan a una gran variedad de obstáculos que complican el proceso de mantener a los dispositivos médicos actualizados corrigiendo las

fallas de los sistemas y manteniendo adecuadas protecciones anti-virus. Entre estos obstáculos se incluyen:

- El gran esfuerzo requerido, en términos de asignación de recursos, para manejar el creciente número de dispositivos médicos interconectados.

- Retrasos en la disponibilidad de actualizaciones del sistema operativo por la necesidad de los fabricantes de probar y validar los cambios antes de implementarlos.

- La imposibilidad para aplicar los cambios a los sistemas operativos y el software anti virus a ciertos equipos médicos (típicamente equipos heredados), en la creencia de que la modificación afectará la funcionalidad del equipo o anulará su garantía.

- La necesidad de continuar utilizando equipos con hardware o software muy antiguo, que ya no tiene el soporte técnico del fabricante o bien con fechas de finalización de soporte muy cercanas (Por ej.la decisión de Microsoft de finalizar su soporte para Windows XP está afectando a numerosos equipos en hospitales)

- La necesidad de proteger además otros equipos auxiliares que pueden ser conectados al dispositivo médico. El ejemplo más típico de esto son las laptops, que pueden llegar a ser conectadas para acceder a las historias electrónicas o intercambiar datos. Las mismas deben también estar protegidas con adecuado software antivirus. Como las laptops son móviles, puede ser muy difícil para un hospital controlar su uso, teniendo en cuenta además que las mismas pueden estar expuestas a muchas más amenazas, como, por ejemplo, la conexión a Internet.

- Inconsistente soporte de la industria de tecnología médica. Los fabricantes de dispositivos médicos pueden ayudar a las instituciones de salud en sus esfuerzos de protección apoyando activamente las medidas de seguridad electrónica en el diseño y desarrollo de sus equipos. Actualmente, la FDA recomienda que los pedidos de aprobación de tecnología médica se encuentren acompañados de un resumen del plan para “brindar actualizaciones validadas del software según se requieran a lo largo del ciclo de vida del equipo para continuar garantizando su seguridad y efectividad” (FDA Content of premarket submissions for management of cybersecurity in medical devices:guidance for Industry and FDA staff, Oct.2 2014).

- Inconsistente apoyo de la industria informática. Los productos informáticos que hacen interfase con los equipos médicos (por ejemplo aquellos diseñados para ayudar a los hospitales a integrar la información provista por los equipos a las operaciones diarias y la historia clínica) pueden no estar diseñados con los mecanismos de seguridad suficientes como para proteger a los equipos de riesgos cibernéticos. Las instituciones de salud necesitan evaluar la protección que ofrecen estos productos y tomar las debidas precauciones cuando se implementan.

Otra medida clave de ciberseguridad consiste en la protección de los datos de pacientes que son recolectados y transmitidos a través de dispositivos y sistemas médicos. Si bien la violación de la confidencialidad no amenaza directamente la salud de los pacientes, es un tema que merece ser abordado en los programas de seguridad informática institucionales. Laptops, dispositivos USB y teléfonos celulares son utilizados cada vez más para intercambiar información o acceder a datos provistos por los sistemas y dispositivos médicos. Como estos equipos pueden fácilmente perderse, robarse o ser usados por personas no autorizadas, es importante que las instituciones consideren medidas de seguridad tales como el encriptado y el control de accesos para éstos como para otros dispositivos que pueden acceder y almacenar información de los pacientes.

Recomendaciones

Los departamentos de ingeniería clínica, de sistemas y de administración de riesgos deberían colaborar en la revisión y de ser necesario, en la actualización de las

normas y procedimientos de seguridad electrónica. Entre los pasos que las instituciones de salud pueden tomar para minimizar las amenazas a la ciberseguridad se incluyen:

- Evaluación proactiva de los riesgos de seguridad informática de los equipos médicos, trabajando si corresponde con sus fabricantes.

- Mantenerse al día con las últimas actualizaciones de los sistemas operativos y software antivirus. Este esfuerzo se ve facilitado si se exigen requerimientos de seguridad en el proceso de compra de nuevos equipos y haciendo que la seguridad informática sea un factor importante en el proceso de selección, como así también incluyendo cláusulas en los contratos de compra respecto a la actualización del sistema operativo y software antivirus

- Limite el acceso de la red a los dispositivos médicos a través de firewalls. Más aún, considere limitar la cantidad de y tipo de equipamiento médico con acceso a las redes de la institución. Sólo a aquellos equipos que requieren dicha conexión. Esta selectividad puede acarrear costos adicionales, pero brindan mayor seguridad que los bloqueos habituales a través de firewalls y se recomiendan para infraestructura crítica.

- Audite los accesos (log-in) a todos los equipos médicos y asegúrese de establecer y de que se cumpla una adecuada política con respecto a las claves de usuario.

- Desarrolle un proceso para monitorear y reportar eventos y amenazas a la seguridad electrónica. Los incidentes que afectan los equipos médicos y los sistemas informáticos (ej historias clínicas electrónicas) deberían ser reportadas a entidades como la FDA o ECRI Institute. Si además existen razones para sospechar que el evento se debe a un ataque malicioso del evento debería ser denunciado a las autoridades policiales que correspondan.

Los programas de seguridad informática deberían estar en paralelo con o aún incorporados a los programas de seguridad informática de la organización. Los planes deberían incluir:

- La evaluación de los riesgos de seguridad electrónica basados en el inventario institucional de equipos médicos y sistemas y la infraestructura de red.

- Protecciones confiables contra amenazas cibernéticas

- Un plan de respuesta y mitigación ante la eventualidad de una infiltración e infección del sistema.

10. Sobrecarga de recordatorios de fallas y alertas de seguridad para equipos electrónicos

Los equipos médicos pueden presentar todo tipo de problemas, desde algunos con muy baja prioridad hasta otros potencialmente fatales. Estos problemas pueden dar origen a advertencias o alertas de seguridad por parte de los fabricantes o de organizaciones como la FDA o ECRI Institute. Las mismas buscan alertar a las instituciones sobre problemas identificados antes de que ocurran nuevos incidentes. Sin embargo, las alertas por sí solas no protegen a los pacientes de daños; las instituciones de salud deben responder apropiadamente a estas alertas para evitar daños prevenibles.

Dos casos investigados por ECRI Institute ilustran este punto. En ambos casos, el fabricante emitió un comunicado acerca de la necesidad de actualizar el software. Y en ambos casos la institución recibió esta noticia pero el staff no realizó la actualización. (A esto se sumó que el personal de mantenimiento preventivo de sistemas no verificó que se estaba utilizando la versión vieja). Estos descuidos comprometieron significativamente la seguridad de los pacientes. En un caso, el paciente fue sometido a un tratamiento inapropiado. En el otro, el descuido determinó que el equipo se recalentara, dañándolo severamente y poniendo en riesgo de lesiones inmediatas al paciente y al personal.

Cuando estos incidentes aparecen, el manejo de las advertencias y alertas de seguridad (su recepción, distribución, respuesta y documentación) es más que una tarea administrativa; es una función crítica para la seguridad de los pacientes. Un programa bien diseñado y efectivo de administración de alertas de seguridad debe ayudar a que el personal de sistemas identifique y aborde el problema de los dispositivos defectuosos (y otras fuentes de peligros o dificultades con la tecnología médica) antes de que los pacientes sean dañados.

Si bien los programas de alerta y advertencia de los fabricantes son comunes, una de las principales preocupaciones de los especialistas en seguridad es que algunos programas hospitalarios no puedan seguir el ritmo del creciente número de alertas y advertencias que se emiten por año. La FDA informó que el número de alertas sobre dispositivos médicos publicadas se duplicó entre los años 2003 y 2013 (de 604 a 1.190).

Para las instituciones de salud, esto significa que los procesos que funcionaban hace una década pueden no ser suficientes para manejar el actual volumen de advertencias. Se necesitan mayores esfuerzos o sistemas más robustos para verificar que cualquier equipo defectuoso sea identificado y que se han dado los pasos necesarios para remediar el problema.

Otra consideración adicional radica en saber si el programa de administración de alertas de seguridad es lo suficientemente abarcativo como para cubrir todos los escenarios posibles. Los siguientes son algunos de los desafíos particulares que se plantean.

- Los implantes, que muchas veces son "stockeados" en consignación (y por lo tanto no aparecen en la historia de compras hasta su colocación). Por lo tanto, una alerta sobre un producto en particular puede perderse si, por ejemplo, la principal forma de identificar los productos afectados se basa en la búsqueda del historial de compras de la institución)

- Las actualizaciones de software, que se han transformado en una preocupación creciente con la proliferación de dispositivos controlados de esa manera. De hecho, el 15 % de todas las alertas de la FDA entre 2010 y 2012 fueron sobre diseño de software. Tanto los fabricantes de equipos como el personal del hospital han expresado la dificultad que tienen para enterarse de la disponibilidad de actualizaciones de software (ej: muchas veces las noticias no llegan a las personas que debieran saber)

- Los sistemas de equipos integrados, como por ejemplo las computadoras que se utilizan para planificar tratamientos de radioterapia y los aceleradores lineales, que deben intercambiar información a través de interfases, a veces entre componentes de distintos fabricantes. Debe tenerse cuidado cuando se implementan cambios en uno de los sistemas (aj: actualización de software), verificando que estas modificaciones no afecten negativamente el intercambio de datos a través de la interfase.

- Equipamientos que requieren arreglos temporarios hasta que el arreglo permanente se encuentre disponible. La comunicación de la necesidad del "parche" y el entrenamiento del personal relevante en el nuevo procedimiento puede ser un proceso complicado.

- Equipos alquilados, prestados o que no pertenecen al hospital (ej: equipamiento quirúrgico perteneciente a un cirujano independiente). Dicho equipo puede no aparecer en el inventario del hospital.

- Equipamiento de internación domiciliaria bajo el control del hospital. Estos quipos pueden no ser tenidos en cuenta si, por ejemplo, no existe un Comité que controle activamente todos los dispositivos de la institución.

Las deficiencias en el manejo de estas alertas de seguridad pueden hacer que no se corrijan problemas identificados por la industria en equipos médicos pudiendo potencialmente dañar a los pacientes.

Recomendaciones

ECRI Institute recomienda que revise su proceso para identificar alertas de seguridad y advertencias sobre productos médicos, haciendo que las recomendaciones lleguen al personal correspondiente, documentando las

medidas correctivas tomadas. Entre los elementos de un programa efectivo se incluyen:

- Apoyo ejecutivo. Una orden proveniente de las más altas autoridades de la institución facilitará la colaboración entre el personal que maneja las alertas y los expertos clínicos que utilizan, mantienen o administran las tecnologías en cada servicio, reduciendo así la posibilidad de que las alertas se pierdan.

- Considerar al manejo de estas alertas como una actividad prioritaria para la seguridad de los pacientes y no como un simple proceso administrativo de rutina.

- Desarrollar un circuito cerrado, que además de distribuir las alertas, incluya la confirmación de que estas alertas han sido recibidas por una persona responsable y la documentación de las medidas correctivas.

- Una norma escrita especificando, por ejemplo, a quiénes deben distribuirse las alertas recibidas, cómo se procesarán y cómo se documentarán las respuestas a estas alertas.

El fabricante o la organización que emite una alerta puede dirigir la misma a un departamento específico, a un médico en particular u a otros. Por eso, todas las partes deberán estar capacitadas sobre el proceso de dirigir las alertas a la persona o departamento correcto.