NOBLE
COMPAÑÍA DE SEGUROS

1

CELULARES, TABLETS Y DISPOSITIVOS ELECTRÓNICOS PERSONALES EN INSTITUCIONES DE SALUD * Conozca los riesgos

Dr. Fabián Vítolo
Noble Compañía de Seguros

La utilización de teléfonos celulares inteligentes (smartphones), tablets y otros dispositivos electrónicos personales (DEPs) viene aumentado significativamente en los últimos años, en una tendencia que difícilmente se revierta. Cerca del 90% de los 238 médicos que respondieron a una encuesta realizada en 2015 por HIMSS (Health Information and Management Systems Society de los EE.UU) reportaron que utilizaban dispositivos móviles para interactuar con sus pacientes.(1) Otra investigación realizada en ese mismo país reveló a su vez que cerca del 80% de los médicos tienen smartphones y cerca del 50% utilizan sus celulares y tablets con propósitos laborales (2)

Y no son sólo los médicos quienes los utilizan. Una micro-encuesta de 241 enfermeras encontró que cerca del 93% de ellas disponían de smartphones y que el 88% los utilizaba en su trabajo, ya sea para encontrar información sobre medicamentos (73%), para encontrar información sobre enfermedades (72%) o para comunicarse con colegas (69%).(3) A esto se suma que la mayoría de los pacientes también tienen sus propios DEPs. Pew Research (2015) reportó que el 64% de los norteamericanos adultos tienen celulares inteligentes y el 42% tablets, y que la mayoría tiene la expectativa de poder utilizarlos durante su estadía en instituciones de salud.(4) Nuestro país no es muy distinto. Aunque la Argentina cerró 2014 con una reducción en las ventas de teléfonos, el parque de equipos viró decididamente hacia los teléfonos inteligentes: según estimaciones de la consultora Carrier y Asociados, el 84 por ciento de los teléfonos celulares vendidos en el país en 2014 fue un smartphone. En 2013 los teléfonos inteligentes conformaban sólo el 56 por ciento de las ventas.(5)

Los dispositivos electrónicos personales (DEPs) tienen muchas funciones que los hacen muy útiles para la atención médica. Ayudan a reforzar la comunicación del equipo de salud, ofrecen un rápido acceso a información sobre el paciente o a material de referencia y promueven la satisfacción de los pacientes internados permitiendo que ellos y quienes los visitan se mantengan conectados con su vida de todos los días. Los médicos también pueden usar los DEPs para acceder a la historia clínica electrónica de sus lugares de trabajo, para monitorear signos vitales de sus pacientes y para promover la educación en salud de sus pacientes.

Sin embargo, los DEPs también generan una serie de riesgos que deben ser abordados: problemas de seguridad y confidencialidad, distracciones, ruidos molestos, contaminación cruzada, e interferencia electromagnética, entre otros.

Seguridad y Confidencialidad

La capacidad que tienen los dispositivos electrónicos personales (DEPs) de acceder, procesar y almacenar datos sobre los pacientes trae aparejada una gran variedad de riesgos regulatorios y legales que deben ser analizados para garantizar que la información contenida en la historia electrónica sea protegida de manera razonable y apropiada. La falta de protección del secreto médico y la integridad de las historias expone a los profesionales y a las instituciones a violaciones de la ley de derechos del paciente.

** Basado en el artículo "Personal Electronic Devices in Healthcare". ECRI Institute 17 Sept. 2015. Healthcare Risk Control. Guidance. www.ecri.org. Traducción y adaptación a nuestro medio: Dr. Fabián Vítolo. NOBLE Cía de Seguros.*

La privacidad y confidencialidad de la información de salud contenida en las historias puede verse comprometida de diversas formas:

- Revelación involuntaria de información de salud protegida electrónicamente a usuarios no autorizados.
- Robo o pérdida de un dispositivo electrónico personal que contenía información de la historia clínica de los pacientes.
- Personal que transmite información protegida de la historia electrónica por una red Wi-Fi insegura.
- Personal que postea información protegida de los pacientes en redes sociales.
- Personal, pacientes o visitantes que inadvertidamente exponen a la red de la institución a virus informáticos que destruyen datos.
- Acceso al sistema informático de la institución por parte de individuos no autorizados.
- Personal o médicos que reenvían un correo no encriptado con información del paciente de su cuenta organizacional a su cuenta personal, la cual no cuenta con los mecanismos de seguridad informática que sí tiene la institución donde trabajan.

Además, otras funciones propias de los DEPs, como los mensajes de texto, las fotos, videos y grabaciones pueden comprometer la privacidad:

Mensajes de texto:

Los mensajes de texto (SMS) se han transformado en un medio muy común de comunicación para muchos profesionales de la salud debido a su inmediatez y eficiencia. Desafortunadamente, los mensajes de texto tradicionales también son inseguros, y exponen a las instituciones de salud a riesgos legales y regulatorios. Los SMS que contienen información sobre los pacientes pueden ser leídos y reenviados a cualquier persona, y permanecen en los servidores de los prestadores de internet y en los celulares de quienes los reciben o envían por tiempo indefinido. En los Estados Unidos, una sola violación de la seguridad de las comunicaciones ha dado origen a multas de hasta US$ de 50.000, y las violaciones repetidas pueden dar lugar a multas que llegan al millón y medio de dólares. (6)

La Joint Commission específicamente prohíbe los mensajes de texto tradicionales en el ámbito de la salud. En respuesta a una pregunta realizada en la sección de dudas frecuentes (FAQ), el organismo sostiene lo siguiente:(7)

"No resulta aceptable que los médicos u otros profesionales de la salud, envíen indicaciones médicas por SMS para pacientes del hospital u otros ámbitos de atención de la salud. Este método no permite verificar la identidad de la persona que envía el mensaje de texto y no hay forma de quedarse con el mensaje original como una forma de validación de lo que se ingresa a la historia clínica"

En abril del 2015, la Joint Commission explicó con más detalle su postura respecto a los SMS en la atención de la salud: (8)

- Los mensajes con temas relacionados a la atención de la salud deben ser rastreados, abiertos y respondidos. Si bien el rastreo de los mensajes de texto no es un problema, sí lo es la verificación de que fueron abiertos y de que se accionó a partir de los mismos.
- Los textos poco claros o la utilización de abreviaturas pueden generar problemas de comunicación y confusiones que lleven a retrasar potencialmente los tratamientos.
- La recolección y verificación de los números de teléfono de los miembros del staff al inicio de cada turno es extremadamente engorrosa y hace perder tiempo.
- No hay forma de saber las razones por las cuales una persona no ha respondido al mensaje de texto o si efectivamente lo ha recibido.
- Proteger y ocultar información personal de los pacientes (estado, resultados de laboratorio o identidad) es muy difícil en estas comunicaciones rápidas, y es posible que el teléfono (y por

extensión la información que contiene), termine en las manos de un usuario no autorizado, exponiendo al hospital a litigios.

- La función de autocorrección de los mensajes de texto puede generar confusiones, o peor, derivar en la transmisión de una información incorrecta (ej: prescripción de una medicación o dosis inapropiada)

- Los mensajes de texto generalmente escapan al control del Departamento de Informática Médica de las instituciones y pueden ser fácilmente abiertos por personas no autorizadas.

La Joint Commission puntualiza que existe un número de aplicaciones de smartphones específicamente diseñadas para comunicaciones urgentes o críticas que separan los mensajes urgentes y relacionados con el trabajo de los mensajes privados no urgentes, y que pueden servir como buenas alternativas al SMS. También ha establecido una serie de recomendaciones para garantizar un sistema de comunicación privado y seguro, entre ellas: (6)

- Centros de datos protegidos fuera o dentro del sitio (basados en la nube) que tengan un alto nivel de seguridad física, como así también normas para revisar de manera periódica los controles.

- Encriptación de los mensajes, tanto en tránsito como en su almacenamiento.

- Normas y procedimientos que distingan entre situaciones en las cuales resulta apropiado enviar un mensaje de texto y aquellas que ameritan una comunicación telefónica.

- Validación de la identidad del receptor que le permita saber al emisor si el mensaje ha sido recibido, por quién y cuándo.

- Controles de auditoría que generen un registro de cualquier actividad que contenga información de salud de los pacientes con capacidad de archivar y recuperar la información y la posibilidad de monitorear el sistema.

- Entrenamiento al personal acerca del uso apropiado de los mensajes de texto.

Fotografías, filmaciones y grabaciones de voz

Las imágenes, videos y audios tomados con un dispositivo electrónico personal pueden, dependiendo de su contenido, ser considerados parte del secreto médico protegido, y generar problemas si el paciente puede ser identificado por personas no autorizadas. A esto se suma el hecho de que muchos pacientes graban de manera encubierta sus conversaciones con los médicos o distintas situaciones mientras se encuentran en la institución. Estas grabaciones pueden ser sacadas de contexto y difundidas en redes sociales, exponiendo a los profesionales y a los establecimientos de salud a publicidad adversa y a potenciales litigios. Hace unos años, en los EE.UU, un paciente dejó inadvertidamente abierto el grabador de su celular mientras le hacían una colonocopía con sedación. Durante el procedimiento, el anestesiólogo realizó comentarios peyorativos sobre el paciente que quedaron grabados en su celular. El paciente entabló una demanda por daños y perjuicios contra el gastroenterólogo y el anestesista. La sentencia obligó a ambos profesionales a resarcirlo en US$ 500.000.(9)

Distracciones

Las distracciones e interrupciones en el ámbito de la atención de salud son una amenaza para le seguridad de los pacientes y del personal por igual. Sólo como ejemplo, entre enero de 2010 y mayo de 2013 la Oficina de Seguridad del Paciente de Pennsylvania (Pennsylvania Patient Safety Authority), recibió 304 reportes de eventos adversos en quirófanos, en los cuales el principal factor contribuyente fueron las distracciones e interrupciones.(10) Si bien la mayoría de estos reportes no especifican si algún Smartphone u otro tipo de dispositivo electrónico personal estuvo involucrado en estos eventos, distintos estudios han demostrado que cualquier cosa que distraiga o interrumpa a los profesionales genera riesgos para la seguridad de los pacientes.

La creciente presencia de DEPs en las áreas de atención de pacientes hace que sea muy fácil para el personal ceder a la tentación de seguir asuntos personales revisando sus mensajes y correos o chequeando redes sociales mientras están en el trabajo. Existen reportes

de personal utilizando sus celulares o tablets aún durante cirugías para realizar llamadas personales, enviar mensajes de texto o mails, ver redes sociales o comprar en línea. Estas distracciones pueden llevar a un aumento en el número de errores. Veamos los siguientes ejemplos (casos reales)

- Durante una cirugía cardíaca a cielo abierto, un anestesiólogo estaba usando su Smartphone para postear comentarios en Facebook y presuntamente no habría advertido los bajos niveles de oxígeno en sangre de su paciente, quien posteriormente falleció.(11)

- Cuando estaba ingresando vía Smartphone una prescripción electrónica para discontinuar una terapia anticoagulante en un paciente, un residente fue interrumpido por un mensaje de texto personal. El residente respondió al SMS y se olvidó de completar la indicación. A consecuencia de esto, la medicación anticoagulante continuó durante varios días, y el paciente desarrolló una condición que requirió una cirugía cardíaca a cielo abierto. (12)

Una encuesta realizada en 2010 a 439 perfusionistas encontró que el 55,6% y el 49,2% de quienes respondieron admitieron utilizar sus celulares o mensajear respectivamente durante cirugías de by-pass coronario, si bien más de la mitad de los mismos consideraba que eran prácticas siempre inseguras.(13)

En otra encuesta, más de la mitad de 112 profesionales del área de seguridad encuestados consignaron que habían recibido reportes relativos a personal de quirófano distraído por dispositivos móviles durante la cirugía, y el 41% había sido testigo presencial de este tipo de conductas. Más aún, 6 de las personas que respondieron indicaron que el uso de dispositivos móviles personales estuvo ligado a eventos adversos ocurridos en sus hospitales, incluyendo un error de sitio quirúrgico.(14)

Las distracciones digitales también pueden afectar negativamente la relación médico-paciente. Concentrarse más en el celular o en la tablet que en la persona que se tiene enfrente puede hacer que ésta se cuestione la calidad de su cuidado y se pregunte si está recibiendo toda la atención que merece. Los médicos más concentrados en las pantallas que en las personas suelen perderse muchos datos acerca de la condición de sus pacientes.

Y no son sólo los profesionales de la salud quienes se distraen. Los pacientes también pueden ser distraídos por sus celulares durante el interrogatorio y el examen físico, lo que puede resultar en problemas de comunicación o mayor tiempo para confeccionar su historia clínica.

Ruido

Los pacientes internados, además de quienes los cuidan o visitan, suelen utilizar sus celulares, tablets o laptops para escuchar música, jugar o acceder a entretenimientos online. La utilización de estos DEPs impacta negativamente sobre el nivel de ruido de los hospitales, que de por sí suele ser alto.

La atención de la salud requiere de un ambiente tranquilo y silencioso, ya que los pacientes necesitan dormir bien para recuperarse. Distintos estudios han demostrado que el aumento del nivel de ruido en los hospitales puede llevar a aumentos de la presión arterial y de la frecuencia cardíaca de los pacientes, además de tener una influencia negativa sobre su tiempo de convalecencia.(15)

De hecho, el ruido molesto es uno de los principales problemas que remarcan los pacientes en las encuestas de satisfacción. En una de encuesta 2012, por ejemplo, sólo el 60% de los encuestados sostuvo que el área fuera de su habitación se mantenía tranquila durante la noche.(16) Como actualmente Medicare basa parcialmente sus pagos en base al resultado de las encuestas de satisfacción, este tema está captando cada vez más la atención de los administradores.

Los pacientes no son los únicos afectados por el ruido excesivo: investigadores encontraron que los trabajadores de la salud expuestos a diferentes niveles de ruido durante sus horas de trabajo en una unidad coronaria, tenían mayores niveles de estrés y tensión durante los períodos acústicos “malos” que durante los períodos acústicos “buenos”.(15) Por supuesto, el ruido también puede contribuir a la distracción de los prestadores.

Seguridad informática

Cualquier dispositivo capaz de acceder a la red del hospital puede servir de vehículo para la transmisión de virus informáticos, haciendo al sistema más vulnerable y abriendo la posibilidad a brechas de seguridad. Como cada vez son más los dispositivos inalámbricos (incluyendo DEPs y equipos médicos) que pueden acceder a las redes del hospital, el peligro para la seguridad informática es cada vez mayor. Según un estudio realizado en 2015 por el Ponemon Institute, un centro que investiga políticas de privacidad y de protección de datos, más del 90% de las organizaciones de salud encuestadas (90), admitieron que habían tenido brechas y violaciones en sus sistemas, con pérdida de datos.(17) El 40% reportó que habían tenido más de de cinco brechas en un lapso de dos años. Los investigadores estiman que el costo promedio de una brecha de seguridad con pérdida de datos para una organización de salud es de aproximadamente 2,1 millones de dólares.

También generan preocupación los intentos maliciosos de hackers que buscan ingresar a los sistemas de los hospitales para sacar información, obtener ilegalmente recetas de narcóticos, robar identidades médicas o ingresar reclamos falsos. El Ponemon Institute sostiene que, en el año 2015, la causa raíz más reportada de fugas de información y accesos no autorizados a las base de datos fueron los ataques criminales, más que los equipos robados o perdidos (17)

Otro estudio llevado a cabo por el SANS Institute analizó datos de inteligencia provistos por Norse, un distribuidor de soluciones informáticas a problemas de seguridad. Los investigadores encontraron que entre septiembre de 2012 y octubre de 2013, 375 organizaciones de salud de los Estados Unidos tenían sus sistemas infectados.(18) Muchas no habían detectado sus compromisos ni reconocido las advertencias del equipo de inteligencia de Norse. Un número significativo de brechas eran el resultado de no tomar medidas de seguridad básicas (ej: no cambiar la credencial por default del firewall)

Riesgos de contaminación cruzada

Además de los virus electrónicos, los microorganismos "tradicionales" también
pueden hacer que los celulares y tablets sean inseguros. Numerosos estudios han demostrado que los DEPs son excelentes caldos de cultivo para una gran variedad de virus y bacterias; su existencia en el ámbito del cuidado de la salud conlleva siempre el riesgo de contaminación cruzada. La combinación de usuarios que constantemente manipulan sus celulares, el calor producido por los mismos aparatos, y el hecho de que generalmente se guardan en lugares oscuros como bolsillos, carteras o maletines, generan las condiciones óptimas para el crecimiento de los microorganismos que se encuentran típicamente en la piel.(19)

Un estudio de 2012, por ejemplo, aisló una muestra total de 179 cultivos positivos de una muestra de 183 celulares del personal de la salud en un hospital.(20) Entre otros patógenos, los autores identificaron 17 especímenes de *estafilococo aureus meticilino resistente* y 20 de *escherichia coli* productoras de beta lactamasa de espectro extendido. Otros investigadores cultivaron muestras de 106 celulares de médicos, encontrando que el 93,4% tenían gérmenes gran positivos y que el 21,7% tenían gran negativos. Cuando preguntaron a los dueños de estos celulares cada cuánto los limpiaban, el 17% de los médicos reportó no limpiarlos nunca. El 46% los limpiaba entre una vez por año y todos los meses y sólo el 34,8% declaró limpiarlo en forma diaria o semanal. (21)

Pero el riesgo no proviene solo de los médicos, enfermeras y personal de salud. Un estudio de 2011 examinó 200 teléfonos celulares, 67 de los cuales pertenecían a empleados de la institución y 133 a pacientes, acompañantes y visitas. El estudio encontró mayor cantidad de celulares colonizados en el grupo de pacientes (39,6%) que en el grupo de los trabajadores de la salud (20,6%), incluyendo un mayor número de microorganismos multirresistentes. (22)

Interferencia electromagnética (EMI)

En el pasado, la posibilidad de que la interferencia electromagnética (EMI, por sus siglas en ingles), pudiera afectar el funcionamiento de equipos médicos cercanos era una verdadera preocupación. Por esta razón, ECRI

Institute (ONG dedicada a la seguridad del paciente y evaluación de tecnología médica), abogó por restricción al uso de DEPs en aéreas con mucho equipamiento electrónico (como las terapias intensivas y los quirófanos). Hoy se sabe que, si bien puede existir EMI, principalmente con equipos médicos viejos, el riesgo de que esta interferencia pueda afectar negativamente la seguridad de los pacientes es bajo. Son varios los factores que han ayudado para reducir este riesgo, incluyendo los actuales requerimientos de diseño de los equipos médicos, que especifican los patrones que deben incorporarse para protegerlos de las interferencias electromagnéticas, junto con desarrollos tecnológicos que permiten que los celulares operen con menor potencia de salida. Por ello, actualmente ECRI Institute considera como rígidas y generalmente innecesarias las políticas que prohíben el uso de celulares y tablets en ciertas áreas del hospital sobre la base exclusiva de la posibilidad de interferencia electromagnética.(23)

Recarga de celulares y DEPs

El intento de recarga de celulares, tablets y demás DEPs en los hospitales también puede generar peligros. Existe la posibilidad de que los pacientes o visitantes utilicen fuentes de energía que están diseñadas para otros propósitos (Ej: puertos USB de quipos médicos) o, peor aún, que desconecten algún equipo médico crítico para acceder a un enchufe.

Limitaciones de la pantalla

Los médicos y enfermeras pueden querer utilizar sus celulares para acceder a la historia clínica electrónica o bien utilizar ciertas apps para ver, por ejemplo, imágenes de radiología. Si bien esto aparece como deseable en teoría, el menor tamaño de la pantalla del celular puede, en la práctica, hacer que los médicos pasen por alto información importante o que no adviertan ciertas cosas que habrían visto en una pantalla más grande o con mejor resolución.

Aumento del tráfico en la red Wi-Fi

Cuanto más son los equipos que acceden a la red Wi-Fi de la institución, mayores son las posibilidades de que se sature la red. Para poder cumplir con la creciente demanda sin que se afecten aplicaciones online que son críticas (ej: telemetría en tiempo real que operan con frecuencias Wi-Fi), se pueden llegar a requerir upgrades de infraestructura costosos.

Plan de Acción

1. Desarrolle una norma respecto al uso de DEPs en su institución
2. Proteja la privacidad de las pacientes y aborde las amenazas a la seguridad informática
3. Limite el uso de celulares en áreas clave
4. Minimice el riesgo de contaminación cruzada
5. Manténgase alerta a signos de interferencia electromagnética
6. Incluya el tema de la recarga de DEPs en la política institucional
7. investigue si las pantallas de los DEPs tienen limitaciones
8. Garantice la disponibilidad de adecuados recursos de red

1. Desarrolle una norma respecto al uso de celulares y otros DEPs en su institución

Para manejar los riesgos asociados a los dispositivos electrónicos personales, las organizaciones deberían establecer políticas que regulen la utilización de los mismos en el ámbito de atención. Pese a esto, sólo el 57% de las instituciones encuestadas por HIMSS en 2015 reportaron que tenían normas y procedimientos activos al respecto. Un 33% contestó que desarrollarían una política próximamente. (1)

En los Estados Unidos, la Oficina de Coordinación Nacional de Tecnologías Informáticas en Salud (ONC) ha compilado una gran variedad de recursos acerca de la protección de la privacidad y seguridad de la información de salud cuando se utilizan dispositivos móviles. La página web de la ONC brinda definiciones relevantes para la seguridad de los dispositivos móviles, junto con tips e información para proteger la seguridad de los datos contenidos en las historias clínicas en los teléfonos celulares. También publica respuestas a preguntas frecuentes y material educativo, incluyendo un listado de los siguientes cinco pasos que las organizaciones de salud pueden seguir para supervisar el uso de los celulares y tablets utilizados por los pacientes y profesionales.(24)

1. Defina si su organización permitirá el uso de dispositivos móviles para acceder, recibir, transmitir o almacenar información acerca de la salud de los pacientes y si considerará a estos dispositivos como una parte más de los sistemas y redes internas institucionales.

2. Evalúe la forma en la cual los dispositivos móviles pueden generar riesgos para la información de salud contenida en sus sistemas informáticos (amenazas y vulnerabilidades)

3. Adopte una estrategia de gestión de riesgo sobre el uso de celulares y tablets, incluyendo protecciones que garanticen la seguridad y privacidad.

4. Desarrolle, documente e implemente la política y los procedimientos de su organización sobre el uso de dispositivos móviles y la forma de proteger la información de salud de los pacientes.

5. Capacite a los profesionales y al resto del personal en seguridad de los dispositivos móviles, cómo proteger y asegurar tanto a estos equipos como a la información contenida en las historias electrónicas, y cómo evitar errores cuando se utilizan celulares o tablets en la atención de los pacientes. Asegúrese de que todos los trabajadores conocen las políticas de la institución acerca del uso de dispositivos móviles.

El desarrollo de una política respecto al uso de dispositivos móviles que tenga sentido para su institución es fundamental para proteger a la misma de riesgos. Estas políticas deben balancear las necesidades del personal de salud, de los pacientes, de los visitantes y de la institución, definiendo claramente cuándo, dónde y con qué propósitos pueden utilizarse los dispositivos personales. La normativa debería incluir una clara definición sobre la propiedad de los datos (qué datos son considerados como propios de la institución y cuáles son propiedad del usuario del dispositivo.) También deben definir a qué se considera información sensible y protegida. Para ser exitosas, las políticas necesitan tener el respaldo de las autoridades y la colaboración de los usuarios, incluyendo al personal clínico y administrativo, médicos independientes, pacientes, proveedores y visitantes. Puede considerarse la inclusión de estas políticas en los contratos que firma la institución con las distintas partes.

Forme un Comité Multidisciplinario

El primer paso para establecer una política de DEPs consiste en reunir un comité multidisciplinario. En la mesa de discusión deberían sentarse representantes de los siguientes departamentos o grupos:

- Informática. El equipo de informática puede ofrecer experiencia acerca de la forma en la que el personal está utilizando los DEPs y de cómo se los puede integrar con el sistema informático actual. Los técnicos pueden ayudar a garantizar que las actuales redes, servidores y resto de quipos pueda soportar la incorporación de dispositivos personales y determinar si se pueden proteger de manera efectiva sus sistemas contra virus y ataques informáticos.

- Enfermería. Los líderes de enfermería pueden dar una idea acerca de la actual carga de trabajo, opinar sobre cómo el uso de DEPs puede afectarlos y ayudar para ver la mejor forma para que la política que se proponga se adapte fácilmente a los procesos o los mejore.

- Médicos. Los líderes médicos pueden evaluar la voluntad de sus colegas para adoptar la nueva política y promover los cambios que se propongan.

- Seguridad del paciente. Los miembros del equipo de seguridad del paciente (u otros representantes de pacientes) pueden llevar la voz de los pacientes y asegurar que sus necesidades sean cubiertas.

- Gestión de riesgos. Los responsables de mapear y gestionar riesgos pueden ayudar a pensar acerca de los potenciales, riesgos y peligros que el uso de DEPs puede conllevar y elaborar planes para identificarlos y mitigarlos,

- Líderes de la organización. Su presencia en este comité ayuda a demostrar el compromiso de la institución con la nueva política

- Gerencia administrativa. Ayuda a elaborar el presupuesto del proyecto.

Establezca normas y procedimientos respecto al uso de dispositivos móviles

Una de las primeras tareas del Comité será decidir si autorizará el uso de dispositivos móviles en el ámbito del trabajo. En general, las políticas muy restrictivas son muy difíciles o imposibles de cumplir y no funcionan (una prohibición total que es continuamente violada es menos efectiva que una prohibición parcial que es cumplida de manera consistente).

La mayoría de las instituciones norteamericanas se están alejando de las prohibiciones generalizadas, considerándolas muy ineficientes. Basándose en encuestas realizadas a lo largo de los años, ECRI Institute ha encontrado que el porcentaje de instituciones que prohíben el uso de celulares personales ha declinado con el tiempo, yendo de un 19% que las prohibían en todas las áreas en 2004 a un 4% que sólo las prohíbe en áreas altamente equipadas en 2013.(25)

Muchos gobiernos concuerdan en que los dispositivos móviles no deben ser prohibidos totalmente. El Departamento de Salud Británico, por ejemplo, publicó guías al respecto en 2009, recomendando que se les permita a los pacientes el uso más amplio posible de sus celulares, excepto en áreas donde puedan interferir con equipamiento médico o puedan invadir la privacidad. (26) Japón también flexibilizó las restricciones para el uso de celulares en hospitales y centros de salud, permitiendo su uso en salas de espera y habitaciones.(27)

Por otra parte, una política muy laxa, o la falta una política puede exponer a la institución a una gran variedad de riesgos. Por eso es importante que las organizaciones encuentren un equilibrio entre los dos extremos y documenten la racionalidad de sus decisiones.

Si el comité decide permitir el uso de dispositivos móviles en el hospital, existen tres abordajes básicos: (28)

1. *Dispositivos (celulares/tablets) provistos por la institución:*

En este escenario, la institución compra los equipos y los planes de uso en la expectativa de que los celulares o tablets serán utilizados sólo a los fines laborales. Esta política permite a la organización tener un mayor control acerca de la forma de uso de los dispositivos, ya que el personal de sistemas puede decidir qué aplicaciones pueden ser bajadas, monitorear el equipo, e instalar y actualizar los software de seguridad apropiados.

2. *"Traiga su propio dispositivo":*

Este abordaje permite al personal y a los médicos utilizar sus propios DEPs en la institución para actividades relacionadas con el trabajo. Esta estrategia, cuando se implementa apropiadamente, permite que los médicos y enfermeras utilicen los celulares y tablets con los que se sienten cómodos sin dejar por eso de cumplir con las normas hospitalarias y proteger la seguridad de los contenidos de la historia clínica. Generalmente, esta política contempla la instalación en los equipos de software aprobado por la institución, a través del cual el personal puede comunicarse. Si se elige este abordaje, la institución deberá decidir si estos dispositivos personales podrán conectarse a las redes internas del hospital y a sus sistemas, ya sea en el lugar o de manera remota. Esta política es generalmente la más costo-efectiva, sin embargo su instrumentación no siempre es fácil.

3. *Un abordaje mixto:*

Este abordaje toma elementos de las otras dos políticas descriptas; por ejemplo, estandarizando una marca específica de celulares para los empleados en relación de dependencia, pero permitiendo que los médicos independientes utilicen sus propios equipos.

Cualquiera de estos abordajes puede ser implementado de manera exitosa, pero cada uno requiere de un profundo análisis de los riesgos, de una cuidadosa planificación y de una documentación de las razones que motivan la decisión. La elección institucional reflejará el balance que la misma realiza sobre los costos, esfuerzos gerenciales, nivel de control y de flexibilidad que les permitirá a los usuarios.

2. Proteja la privacidad de los pacientes y aborde las amenazas a la seguridad informática

Minimizando los riesgos para la seguridad informática

Según una encuesta del Ponemon Institute (2015), la negligencia de los empleados en el uso de la historia clínica electrónica es la principal preocupación de las instituciones a la hora de proteger información reservada. El 70% de los encuestados manifestó que éste es el tipo de incidente de seguridad informática más frecuente. (17)

Algunos ejemplos de cómo la negligencia de los usuarios puede generar fugas de información incluyen los siguientes:

- Pérdida o robo de dispositivos electrónicos móviles personales
- Exponer a la institución a virus informáticos al clickear sobre links sospechosos o abriendo mails de fuentes no confiables.
- No utilizando los patrones de seguridad de sus celulares o tablets (ej: claves de usuario, bloqueos.)
- Abriendo información protegida de la historia clínica de sus pacientes en lugares públicos y no protegiendo la información.
- Enviando información de salud protegida de sus pacientes por mails no institucionales o mensajes en redes públicas no seguras.
- Transmitiendo información de los pacientes a través de métodos inseguros y no aprobados (ej: vía mensajes de texto o whatsapps comunes)

Para ayudar a proteger la información contenida en las historias electrónicas institucionales, resulta esencial que quienes gestionan riesgos se familiaricen con los requisitos legales y regulatorios de protección de datos informáticos y desarrollen relaciones colaborativas con los departamentos de legales, de sistemas, de bioingeniería, de recursos humanos y de docencia.

Existe una serie de pasos que las instituciones de salud pueden adoptar para minimizar los riesgos vinculados a la privacidad y seguridad de sus bases informáticas. Entre ellos se incluyen los siguientes:

Utilice medidas de control de acceso: Las medidas de control de accesos protegen contra el acceso de usuarios no autorizados a las redes y sistemas de atención clínica. Estas medidas pueden incluir la institución de una política de claves muy estricta y que los pacientes y visitantes se limiten a utilizar una red Wi.Fi específica para “visitas”.

Requiera que el personal adhiera a los términos de uso institucionales de dispositivos móviles: Las instituciones deberían requerir que su personal clínico y administrativo adhiera expresamente a las políticas de privacidad y seguridad de la información vinculada al uso de dispositivos móviles personales. Sólo aquellos dispositivos que cumplen con los requisitos de seguridad establecidos por la institución deberían poder acceder a aplicaciones sensibles o a información clínica contenida en la red del hospital. Esto aplica tanto para los dispositivos móviles provistos por la institución como para los dispositivos personales que son utilizados con fines laborales, tales como accesos a correos electrónicos corporativos o a la historia clínica.

Desarrolle una política sobre el uso de apps médicas, y mantenga una lista de apps aprobadas para uso del personal

La utilización de aplicaciones móviles (apps) en las instituciones de salud debería ser cuidadosamente monitoreada. Las normas efectivas pueden ayudar a garantizar que las apps médicas sean usadas de manera segura y consistente dentro de la organización, mantengan segura la información de los pacientes y sean confiables para poder ser usadas en la atención. Las instituciones podrían considerar el desarrollo de un listado de apps aprobadas que han sido verificadas como seguras para su uso hospitalario.

En 2014, investigadores de ECRI Institute realizaron una encuesta sobre el uso de apps en hospitales y encontró que cerca del 62% no tenía ninguna política formal sobre esta práctica. Otro porcentaje relativamente importante (28%), sostuvo que no sabía si su hospital tenía alguna disposición al respecto. 50% dijo que no tenían procedimientos para la aprobación de aplicaciones médicas y sólo el 8% confirmó tener normas al respecto. (29)

La FDA ha comenzado recientemente a regular algunas aplicaciones médicas para celulares. Sin embargo, la

mayoría de las apps no cumplen con la definición que el organismo regulador da a los "dispositivos" médicos. Y requiere que estas apps sean utilizadas como un accesorio de equipos médicos regulados o bien que transformen la plataforma móvil en un dispositivo médico regulado.(30) Ante la falta de una regulación por parte de la FDA, las instituciones de salud deben buscar otras formas para evaluar la seguridad y eficacia de estas apps.

Un cierto número de terceras partes está tratando de llenar este vació regulatorio, ya sea evaluando ellas mismas estas apps o brindando recomendaciones elaboradas por los profesionales que las usan. Sin embargo, estas certificaciones no son necesariamente confiables: una compañía de soluciones médicas digitales (Happtique), por ejemplo, tuvo que suspender su programa de aplicaciones de salud luego de que se encontraran brechas de seguridad en dos de sus aplicaciones recomendadas. (31)

Antes de recomendar una aplicación de uso médico, la app debería ser evaluada por personal apropiado. En el proceso de evaluación, las instituciones deberían asegurarse de que las aplicaciones sean de fáciles de usar, provengan de una fuente confiable y estén recomendadas por los usuarios. Si la app será usada para almacenar información protegida de los pacientes, deberá garantizarse el mantenimiento de las claves y el proceso de encriptación.

Resulta interesante conocer las recomendaciones establecidas al respecto por la American Pharmacists Association: (32)

- Conozca cuál es el propósito de la app, y asegúrese de que sea compatible con sus procesos de trabajo.
- Si se utilizará una app con fines médicos, asegúrese de que la información contenida en ella sea precisa, verificable y continuamente actualizada.
- Determine si la información de la app es confiables ya sea investigándola o contactando al programador.

Desarrolle normas para dar de baja y bloquear dispositivos móviles perdidos o robados y reporte estos incidentes

El 90% de las instituciones que respondieron a una encuesta del Ponemon Institute reportaron al menos un incidente de seguridad vinculado a celulares o tablets perdidos o robados.(17) Para manejar estas situaciones, en el caso de dispositivos que puedan contener información de los pacientes, los hospitales deberían establecer protocolos específicos para la notificación de robos o pérdidas de equipos móviles, detallando a quién llamar, en qué horarios, que detalles deberían agregarse. La norma debería recordarse de manera periódica al personal

Capacite a su personal clínico y administrativo en las normas de su institución respecto al uso de dispositivos electrónicos móviles e instrúyalos para que se mantengan alerta ante mails y links sospechosos.

Los virus informáticos pueden infectar los DEPs de distintas formas, de las cuales la más común es el phishing. El phishing es un término informático que denomina un modelo de abuso informático, caracterizado por intentar adquirir información confidencial de manera fraudulenta. El cibercriminal (conocido como phisher), se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea.

Para reducir este riesgo, el personal debe ser instruido sobre las distintas formas por las cuales pueden diseminarse estos virus y advertirles que no abran mails sospechosos. Estos incidentes también deben ser denunciados a través de los canales establecidos.

Garantice los fondos suficientes para su programa de seguridad informática

Uno de los principales obstáculos a los que deben enfrentarse las instituciones de salud cuando abordan el tema de su seguridad informática es la falta de recursos y fondos suficientes. Mantener a un número creciente de equipos médicos interconectados en red actualizados con los últimos softwares de antivirus es un verdadero desafío. De hecho, EL estudio del Ponemon Institute (2015) reportó que el 56% de las instituciones

entrevistadas no creían que su programa de seguridad informática tuviera una adecuada financiación, y sólo el 33% respondió que estaban bien equipados para prevenir o detectar rápidamente cualquier fuga de datos (17). El SANS Institute, por su parte, sostiene que las prácticas y estrategias de seguridad actualmente utilizadas por los hospitales no guardan relación con el volumen de ataques informáticos que sufren.(18) Garantizar que los responsables del mantenimiento de los sistemas y redes del hospital cuenten con los recursos necesarios es vital para proteger la información de las historias clínicas de ciberataques.

Desarrolle y haga cumplir las normas sobre fotografías, videos o grabaciones de voz en el ámbito de su institución

Una clara política, asociada a la capacitación del personal, de los pacientes y visitantes respecto a la necesidad de preservar la privacidad y seguridad puede ayudar a mitigar los riesgos legales de grabaciones o fotografías no autorizadas

Limite el uso de celulares en áreas clave

Para encarar el problema de las distracciones generadas por los celulares y resto de DEPs, las instituciones de salud pueden considerar las siguientes estrategias:

Adopte el concepto de "cabina estéril"

Esto es especialmente útil para evitar distracciones durante la cirugía. Se trata copiar las regulaciones de la aviación civil, que impiden a los pilotos entablar conversaciones o actividades que no estén específicamente relacionadas con el despegue o el aterrizaje (generalmente antes y después de cruzar los 10.000 pies.). Este abordaje promueve la seguridad, limitando desconcentraciones durante partes claves de la operación.(33)

Establezca políticas que restrinjan el uso de DEPs

Considere restringir el uso personal de dispositivos electrónicos por parte del staff durante la atención de los pacientes, especialmente en las áreas de quirófano y terapia intensiva. Una acción de este tipo puede aumentar la productividad y ayudar a reducir la probabilidad de que los dispositivos móviles terminen perjudicando a los pacientes.

Varios hospitales han adoptado alguna de las siguientes medidas para minimizar las distracciones: (33)

- Entrega a sus empleados de dispositivos móviles que sólo pueden utilizarse para el trabajo
- Prohibición del uso de celulares y otros DEPs en el quirófano o en UTI, haciendo de estas áreas "zonas silenciosas"·. Alternativamente, algunas instituciones han restringido el uso de DEPs a ciertas áreas, tales como salas de espera, cafeterías, salas de personal o áreas WI-Fi específicas dentro del hospital.
- Prohibiendo el uso de DEPs para negocios personales durante el horario de trabajo
- Recomendando a los cirujanos y a sus ayudantes que les entreguen sus celulares a la circulante de quirófano durante la cirugía, de forma tal que los teléfonos sean monitorizados en caso de emergencias.

Controle los ruidos

Para minimizar distracciones, también se deben controlar los ruidos producidos por los celulares y demás equipos móviles personales. Por ejemplo, algunos miembros del personal, particularmente los cirujanos, suelen disfrutar escuchando música en sus DEPs mientras operan; sin embargo, esto puede generar distracciones, aún con volúmenes bajos. Un estudio, por ejemplo, encontró que los ruidos de fondo del quirófano pueden disminuir significativamente la capacidad de procesar lo que se escucha, particularmente en presencia de música. (34) Las instituciones podrían evaluar si el nivel de ruidos de sus quirófanos es un factor que pueda incidir sobre la seguridad de los pacientes y, de ser así, buscar la mejor solución para evitar en la medida de lo posible esta y otras distracciones.

Los ambientes silenciosos, con un bajo nivel de ruidos, también ayudan a mejorar la experiencia de los pacientes, permitiéndoles descansar mejor y facilitando su recuperación.

Para abordar el tema del exceso de ruidos vinculados a celulares, tablets o laptops, los hospitales pueden considerar los siguientes consejos:

- Recuerde a los usuarios de dispositivos móviles que mantengan el volumen bajo. (tanto de los ringtones –mejor vibración-, como cuando hablan.) Su tono de voz debería ser similar al que se utiliza en bibliotecas públicas.

- Establezca "horas silenciosas" en el hospital para limitar ruidos cuando los pacientes duermen. El Beth Israel Deaconess Medical Center (Boston), por ejemplo, lanzó una campaña denominada "Quiet at Night" (Silencio por la Noche), que buscó reducir al máximo los ruidos entre las 9 de la noche y las 6 de la mañana. Luego de tres meses de iniciado el proyecto, las encuestas de satisfacción mejoraron: un 13% más de pacientes respondieron "siempre" a la pregunta sobre si el área cercana a su habitación se mantenía silenciosa durante la noche.(35)

Minimice el riesgo de contaminación cruzada

La reducción de la contaminación cruzada a partir del uso de celulares y dispositivos móviles en las instituciones de salud puede ser de muy difícil resolución. Un estudio de investigación sobre la contaminación bacteriana de celulares en hospitales identificó cuatro medidas que permitirían reducir este riesgo: (36)

1. Capacite a los usuarios de celulares y demás DEPs sobre la importancia de una adecuada higiene de manos, incluyendo recordatorios visuales (ej: afiches, folletos, etc), en zonas donde los profesionales se congregan.

2. Establezca estrictas medidas de lavado de manos que estipulen que el personal se deba higienizar las manos antes y después de manipular dispositivos electrónicos móviles.

3. Considere restringir el uso de celulares en áreas de alto riesgo (Ej: quirófano, UTI)

4. Establezca recomendaciones sobre la limpieza de los celulares y resto de DEPs

El establecimiento de políticas que garanticen que el personal, los pacientes y visitantes limpien y desinfecten sus celulares y equipos móviles sobre bases regulares es una recomendación muy común en la literatura. Sin embargo, la desinfección adecuada de estos dispositivos puede ser complicada, sobre todo porque los fabricantes no han desarrollado todavía un criterio uniforme acerca de cuál es la mejor forma de hacerlo. La mayoría de los celulares y tablets del mercado están pensados para la población general, y las instrucciones de limpieza brindadas por los fabricantes no están pensadas para cumplir con los rigurosos métodos de desinfección que se aplican con la mayoría de los equipos médicos. Si bien distintos estudios han demostrado que los paños o toallitas con alcohol isopropílico (37) o alcohol etílico al 70% (38) son muy efectivos en la remoción de la mayoría de los microorganismos de las superficies de los celulares o tablets, su utilización puede hacer caer la garantía de estos dispositivos, ya que la mayoría de los fabricantes desaconsejan su uso por temor a degradar la imagen de la pantalla o de que el líquido infiltre el equipo y lo deteriore.

En ausencia de guías claras de desinfección por parte de los fabricantes, un estudio de 2013 promueve un "paquete de medidas" para desinfectar celulares y otros dispositivos móviles; (39)

1. Utilice un estuche no poroso y resistente al agua, ya sea blando o duro, para proteger el dispositivo, y estandarice su uso en toda la institución.

2. Antes de cada uso, desinfecte el dispositivo con un desinfectante aprobado por la institución.

3. Además de lo establecido en el paso anterior, configure al celular o tablet para que envíe recordatorios a los usuarios para que desinfecten sus equipos de manera regular (ej: cada hora, diariamente, etc)

4. Requiera a los usuarios que se laven las manos antes y después de usar el dispositivo.

Algunas instituciones están explorando el uso de luz ultravioleta como una alternativa para desinfectar estos dispositivos, si bien la misma tiene un costo considerable. Un estudio de 2014 encontró que "la aplicación de luz ultravioleta sobre los dispositivos manuales puede ser una alternativa razonable para desinfectar superficies planas que no pueden ser desinfectadas diariamente utilizando los agentes químicos habituales.(40) Sin embargo, la confiabilidad , practicidad, seguridad y costo-efectividad de esta técnica todavía no está probada y requiere de nuevas investigaciones para poder ser adoptada de manera masiva por la comunicad de control de infecciones. Otras preocupaciones con la luz ultravioleta incluyen la posibilidad de que los dispositivos electrónicos se dañen luego de múltiples exposiciones y problemas de seguridad, como irritación de los ojos y de la piel.

Como mínimo, las instituciones deberían desarrollar políticas instruyendo a su personal para que adhiera a las correctas técnicas de higiene de manos antes y después de utilizar el celular. Esto, junto con la limpieza ocasional del dispositivo con un paño húmedo puede llegar a ser suficiente para reducir el riesgo hasta que los fabricantes desarrollen mejores métodos de desinfección.

Manténgase alerta a signos de Interferencia Electromagnética (EMI)

Si bien el riesgo de interferencia electromagnética (EMI), vinculado al uso de celulares u otros dispositivos ha disminuido bastante, no ha desaparecido por completo, sobre todo con el equipamiento médico más antiguo. El mantenimiento de ciertas restricciones resulta entonces prudente.

Para abordar el riesgo de EMI, ECRI Institute recomienda lo siguiente (22)

- Informe a los usuarios de celulares y DEPs que la interferencia electromagnética puede afectar el funcionamiento de equipos médicos cercanos.
- Instruya a los usuarios para que mantengan una distancia de al menos 1 metro (aprox. un brazo de distancia) de los equipos médicos cuando utilizan su celular o tablet y que eviten apoyarlos sobre la superficie o en contacto con los mismos.
- Instruya al personal a que permanezca alerta a cualquier comportamiento anómalo de equipos médicos que puedan sugerir interferencia electromagnética, especialmente con el instrumental más antiguo.

Recarga de dispositivos, temas de pantalla y sobrecarga de la red Wi-Fi

Incluya la recarga de celulares y dispositivos electrónicos personales dentro de las normas institucionales, y capacite al personal y a los pacientes sobre las mismas

La capacitación del personal y de los pacientes sobre las normas hospitalarias que regulan la recarga de la batería de celulares y equipos móviles personales resulta fundamental para minimizar riesgos potenciales. Deben saber, por ejemplo, cuáles enchufes pueden ser utilizados y cuáles no.

Además, es importante advertirles que no utilicen para recargar sus celulares, tablets o laptops los puertos USB de los equipos médicos. Bajo ciertas circunstancias, esta acción puede tener consecuencias mortales. Un fabricante de máquinas de anestesia difundió que si un teléfono celular u otro dispositivo USB era conectado a alguno de los 4 puertos USB que tenía su sistema, el mismo podía dejar de funcionar, resultando en potenciales eventos adversos serios, como hipoxemia y muerte.(41) El personal de enfermería debería ser instruido para verificar periódicamente que los equipos móviles de los pacientes o de los visitantes no se encuentren enchufados de manera indebida.

Determine si existen limitaciones de pantalla

Quienes gestionan riesgos deberían tomar conciencia de cualquier limitación de pantalla que puedan tener las apps, programas y sistemas que el hospital piensa incluir dentro del listado de "aplicaciones aprobadas". Estas limitaciones pueden incluir información que se pierde en una pantalla más chica o que pierde resolución en un celular o tablet. Si se detectan defectos y aún así la institución decide aprobar estas aplicaciones o programas, se debería advertir a los profesionales sobre

sus limitaciones. Además, si la institución no ha desarrollado una política respecto al uso de aplicaciones médicas, los profesionales deberían estar advertidos de que la pantalla del celular, si bien es muy parecida al del monitor de la computadora, no la reproduce exactamente.

Garantice la disponibilidad de suficientes recursos de red

Las instituciones de salud deberían tener redes de Wi-Fi separadas para invitados y para el manejo de la información clínica, buscando prevenir que una sobrecarga de la red por parte de los invitados termine afectando los sistemas de información clínica de la institución. Las redes deberían ser evaluadas de manera periódica y expandidas según las necesidades de crecimiento de las organizaciones.

CELULARES, TABLETS Y DISPOSITIVOS ELECTRÓNICOS PERSONALES EN INSTITUCIONES DE SALUD

Resumen de recomendaciones

- Establezca un comité multidisciplinario para desarrollar y hacer cumplir una política de dispositivos electrónicos personales que se adapte a las circunstancias particulares de su organización.
- Trabaje con el Departamento de Sistemas para garantizar los adecuados controles para proteger las redes y sistemas informáticos contra accesos no autorizados.
- Requiera que el personal clínico y administrativo adhiera a las políticas privacidad y seguridad de la información vinculadas al uso de dispositivos móviles personales.
- Capacite al personal sobre las distintas formas por las cuales los virus informáticos pueden contaminar sus dispositivos móviles y adviértales que sean cautelosos con los e-mails sospechosos o sitios de internet que tengan contenidos maliciosos
- Establezca una política que defina los usos apropiados e inapropiados de cámaras y otros dispositivos de grabación y de aplicaciones dentro del ámbito de atención.
- Limite las distracciones en el quirófano adoptando el concepto de “cabina estéril” o de “zona libre de interrupciones” durante las fases críticas de la cirugía.
- Considere la adopción de políticas que restrinjan el uso de celulares y dispositivos personales a ciertos períodos de tiempo o áreas específicas (ej: durante los descansos o en zonas WI-Fi establecidas). Considera le distribución de dispositivos móviles provistos por la institución que contengan funciones y apps preinstaladas propias de la función que se desempeña.
- Recuerde a los usuarios de dispositivos electrónicos personales que mantengan bajo el volumen y que sean respetuosos de la privacidad de quienes los rodean.
- Capacite al personal sobre los riesgos de contaminación cruzada asociados al uso de celulares y demás DEPs, e instruya a los cuidadores, pacientes y visitantes a realizar una adecuada higiene de manos antes y después de usarlos.
- Evalúe métodos para desinfectar los DEPs y determine cuál es el que mejor se adapta a su institución. Acomode y adapte esta política a los métodos de desinfección existentes.
- Informe a los usuarios de dispositivos electrónicos personales, incluyendo personal, médicos independientes, pacientes y visitantes), que la interferencia electromagnética (EMI) puede afectar el funcionamiento de equipos médicos cercanos, e instrúyalos para que mantengan una distancia de al menos 1 metro cuando utilizan sus celulares, tablets o demás DEPs .
- Instruya al personal a que permanezca alerta a cualquier comportamiento anómalo de equipos médicos que puedan sugerir interferencia electromagnética, especialmente con el instrumental más antiguo.
- Verifique que sus normas sobre el uso de dispositivos electrónicos personales por parte de los pacientes especifiquen los requisitos para recargarlos dentro de la institución.
- Informe a todos los usuarios de dispositivos electrónicos personales que bajo ningún concepto pueden conectarlos a puertos USB de equipos médicos con fines de recarga.
- Evalúe las limitaciones de pantalla que puedan tener las apps, sistemas y programas de uso médico antes de recomendar su uso en celulares o tablets. En caso de haberlas asegúrese de que el personal las conoce.
- Garantice que la red Wi-Fi para invitados sea distinta de la que se utiliza para las redes de informática médica y demás sistemas, y asegúrese de que el ancho de banda sea el apropiado para cumplir con las necesidades de su institución.

Bibliografía

Este artículo resulta de la traducción parcial y adaptación a nuestro medio del documento "Personal Electronic Devices in Healthcare". ECRI Institute 17 Sept. 2015. Healthcare Risk Control. Guidance. www.ecri.org

Se hace a continuación referencia a los artículos e investigaciones mencionadas específicamente en el documento:

1. Healthcare Information and Management Systems Society (HIMSS). 2015 HIMSS mobile technology survey [online]. 2015 Apr 14 [cited 2015 Jun 3]. http://www.himss.org/2015-mobile-survey

2. In-depth: mobile adoption among US physicians [online]. MobiHealthNews 2014 Apr 17 [cited 2015 Jun 28]. http://mobihealthnews.com/32232/in-depth-mobile-adoption-among-us-physicians

3. InCrowd. Your nurse's doctor on call may be an app [online]. 2015 Jun 8 [cited 2015 Jun 28]. http://www.incrowdnow.com/2015/06/your-nurses-doctor-on-call-may-be-an-app

4. Pew Research Center. U.S. smartphone use in 2015 [online]. 2015 Apr 1 [cited 2015 Sep 1]. http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015

5. La Nacion.com. "La Argentina, un país a puro smartphone. 25 de marzo de 2015. http://www.lanacion.com.ar/1777897-la-argentina-un-pais-a-puro-smartphone

6. Brooks AA. Healthcare texting in a HIPAA-compliant environment: texting speeds communication but could put you at risk [online]. AAOS Now 2012 Aug [cited 2015 Jun 28]. http://www.aaos.org/news/aaosnow/aug12/managing5.asp

7. Joint Commission. Standards FAQ details: texting orders [online]. 2015 Apr 22

8. Pelletier MG. Views from the Joint Commission: to text or not to text? [online]. 2015 Apr 10

9. Jackman T. Anesthesiologist trashes sedated patient—and it ends up costing her [online]. Washington Post 2015 Jun 23 [cited 2015 Jul 13]. http://www.washingtonpost.com/local/anesthesiologist-trashes-sedated-patient-juryorders-her-to-pay-500000/2015/06/23/cae05c00-18f3-11e5-ab92-c75ae6ab94b5_story.html

10. Feuerbacher RL, Funk II KH, Spight DH, et al. Realistic distractions and interruptions impair simulated surgical performance by novice surgeons. Arch Surg 2012 Nov;147(11):1026-30. PubMed: http://www.ncbi.nlm.nih.gov/pubmed/22801787

11. Hawryluk M. Is your surgeon focused on you or his smartphone? [online]. Bulletin (Bend, OR) 2015 Feb 2 [cited 2015 Jun 1]. http://www.bendbulletin.com/newsroomstafflist/2834727-151/cellphones-in-operating-roompose-patient-safety-risks

12. Halamka J. Order interrupted by text: multitasking mishap [online]. WebM&M 2011 Dec [cited 2015 Jun 1]. http://webmm.ahrq.gov/case.aspx?caseID=257

13. Smith T, Darline E, Searles B. 2010 survey on cell phone use while performing cardiopulmonary bypass.Perfusion 2011 Sep;26(5):375-80. PubMed: http://www.ncbi.nlm.nih.gov/pubmed/21593081

14. Patterson P. Smartphones, tablets in the OR: with benefits come distractions. OR Manager 2012 Apr;28(4):1, 6-8, 10. PubMed: http://www.ncbi.nlm.nih.gov/pubmed/22594083

15. Call RB. Sound practices: noise control in the healthcare environment [online]. AIA Acad J 2007 Nov http://www.brikbase.org/sites/default/files/aah_journal_v10_2007_nov_05_0.pdf

16. Landro L. Hospitals work on patients' most-frequent complaint: noise [online]. Wall St J 2013 Jun 10 http://www.wsj.com/articles/SB10001424127887324634304578537350035525538

17. Ponemon Institute. Fifth annual benchmark study on privacy and security of healthcare data [online]. 2015

18. SANS Institute. Health care cyberthreat report: widespread compromises detected, compliance nightmare on horizon [white paper online]. 2014 Feb [cited 2015 Jun 28]. http://pages.norsecorp.com/rs/norse/images/Norse-SANS-Healthcare-Cyberthreat-Report2014.pdf

19. Brady RR, Fraser SF, Dunlop MG, et al. Bacterial contamination of mobile communication devices in the operative environment [letter]. J Hosp Infect 2007 Aug;66(4):397-8. PubMed: http://www.ncbi.nlm.nih.gov/pubmed/17573157

20. Ustun C, Cihangiroglu M. Health care workers' mobile phones: a potential cause of microbial cross-contamination between hospitals and community. J Occup Environ Hyg 2012 Sep;9(9):538-42. PubMed: http://www.ncbi.nlm.nih.gov/pubmed/22793671

21. Khan A, Rao A, Reyes-Sacin C, et al. Use of portable electronic devices in a hospital setting and their potential for bacterial colonization. Am J Infect Control 2015 Mar 1;43(3):286-8. PubMed: http://www.ncbi.nlm.nih.gov/pubmed/25557772

22. Tekerekoğlu MS, Duman Y, Serindağ A, et al. Do mobile phones of patients, companions and visitors carry multidrug-resistant hospital pathogens? Am J Infect Control 2011 Jun;39(5):379-81. PubMed: http://www.ncbi.nlm.nih.gov/pubmed/21624635

23. ECRI Institute. Position statement: policies on the use of smartphones should balance the benefits and the risks. Health Devices 2015 Jun 10.

24. Office of the National Coordinator for Health Information Technology (ONC). U.S. Department of Health and Human Services: Five steps organizations can take to manage mobile devices used by health care providers and professionals [online]. https://www.healthit.gov/providers-professionals/five-steps-organizations-can-take-manage-mobile-devices-used-health-care-pro

25. ECRI Institute. Getting the message: results of our survey on cell phone/smartphone policies [guidance article]. Health Devices 2013 Apr;42(4):126-32.

26. Department of Health, U.K. Using mobile phones in NHS hospitals [online]. 2009 Jan [cited 2015 Jun 29]. http://webarchive.nationalarchives.gov.uk/20130107105354/http:/www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_092812.pdf

27. New guidelines ease restrictions on cellphone use at hospitals [online]. 2014 Aug 19 [cited 2015 Jun 29]. http://www.japantimes.co.jp/news/2014/08/19/national/new-guidelines-ease-restrictions-on-cellphone-use-athospitals/#.VZFfq3nbKpp

28. ECRI Institute. Judgment call: smartphone use in hospitals requires smart policies [guidance article]. Health Devices 2012 Oct;41(10):314-29.

29. ECRI Institute. No policy on staff use of medical apps? You're not alone [guidance article]. Health Devices 2014 Mar 5.

30. U.S. Food and Drug Administration (U.S. FDA): Mobile medical apps [online]. Updated 2014 Jun 4 http://www.fda.gov/MedicalDevices/Productsa

ndMedicalProcedures/ConnectedHealth/MobileMedicalApplications/ucm255978.htm

31. Dolan B: Happtique suspends mobile health app certification program [online]. MobiHealthNews 2013 Dec 13 http://mobihealthnews.com/28165/happtique-suspends-mobile-health-app-certificationprogram

32. Erickson AK. Mobile med apps: what's right for your hospital practice? [online]. 2014 Jan 1 http://www.pharmacist.com/mobile-med-apps-what%E2%80%99s-right-your-hospital-practice

33. Feil M. Distractions in the operating room. Pa Patient Saf Advis [online] 2014 Jun

34. Way TJ, Long A, Weihing J, et al. Effect of noise on auditory processing in the operating room. J Am Coll Surg 2013 May;216(5):933-8. PubMed: http://www.ncbi.nlm.nih.gov/pubmed/23518255

35. Beth Israel Deaconess Medical Center. Reducing noise at night [online]. http://www.bidmc.org/QualityandSafety/EffortstoImproveQualityofCare/QualityandSafetyatWork/~/media/Files/QualityandSafety/2012%20Silverman%20Symposium/ImproveInnovate3/NoiseatNight_12R_2012_Final.ashx

36. Brady RR, Verran J, Damani NN, et al. Review of mobile communication devices as potential reservoirs of nosocomial pathogens. J Hosp Infect 2009 Apr;71(4):295-300. PubMed: http://www.ncbi.nlm.nih.gov/pubmed/19168261

37. Albrecht UV, von Jan U, Sediacek L, et al. Standardized, app-based disinfection of iPads in a clinical and nonclinical setting: comparative analysis. J Med Internet Res 2013 Aug 14;15(8):e176. PubMed: http://www.ncbi.nlm.nih.gov/pubmed/23945468

38. Sumritivanicha A, Chintanavilas K, Apisarnthanarak A. Prevalence and type of microorganisms isolated from house staff's mobile phones before and after alcohol cleaning. Infect Control Hosp Epidemiol 2011 Jun;32(6):633-4. PubMed: http://www.ncbi.nlm.nih.gov/pubmed/21558783

39. Manning ML, Davis J, Sparnon E, et al. iPads, droids, and bugs: infection prevention for mobile handheld devices at the point of care. Am J Infect Control 2013 Nov;41(11):1073-6. PubMed: http://www.ncbi.nlm.nih.gov/pubmed/23816356

40. Petersson LP, Albrecht UV, Sedlacek L, et al. Portable UV light as an alternative for decontamination. Am J Infect Control 2014 Dec;42(12):1334-6. PubMed: http://www.ncbi.nlm.nih.gov/pubmed/25465267

41. ECRI Institute Spacelabs—ARKON anesthesia delivery systems: may enter controlled failed state [accession no. A22147]. Health Devices Alerts 2015 Apr 18.