PHILIPS

Ciberseguridad

Mitos relacionados con la ciberseguridad en la digitalización de los expedientes médicos.

Los datos de los pacientes y los expedientes médicos electrónicos

Las tecnologías de gestión, como los expedientes médicos electrónicos (EMR, por sus siglas en inglés) y los portales en línea para ser usados por los pacientes y los proveedores de atención médica, se están convirtiendo rápidamente en estándares de uso en las organizaciones de atención sanitaria.

Si bien estas herramientas y tecnologías facilitan el acceso y la difusión de la información médica y permiten a los pacientes y a sus familias tomar decisiones mejor informadas sobre su salud, también contienen un gran volumen de información sensible de toda índole, desde fechas de nacimiento y números de identificación personal, hasta información sobre diagnósticos y tratamientos médicos. Como consecuencia, estos datos confidenciales y los sistemas en los que residen se están convirtiendo rápidamente en blanco de los delincuentes cibernéticos.

Afortunadamente, y reconociendo la existencia de la amenaza del delito cibernético, muchos países de América Latina han comenzado a hacer obligatorio el uso de EMRs, como por ejemplo Brasil, donde el objetivo es unificar todos los registros médicos electrónicos de los proveedores de salud del gobierno en un solo sistema para el año 2020. Otros países han experimentado un crecimiento continuo y constante en el uso de EMRs como es el caso de Chile y de Uruguay. Ambos países usan expedientes electrónicos en casi el 75 y el 65 por ciento de los proveedores de atención médica, respectivamente.

La amenaza de la delincuencia cibernética

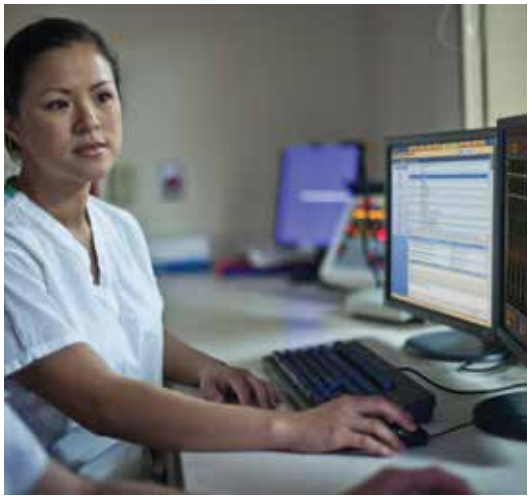
La información relacionada con la salud abarca datos del paciente sobre su estado de salud, sobre los pagos que ha realizado por concepto de atención médica, sobre los servicios de salud que ha recibido, al igual que otros tipos de datos privados de contacto que pueden ser específicamente vinculados a determinadas personas.

Aunque las leyes sobre el manejo de información relacionada con la salud, como por ejemplo la Ley de Portabilidad y Responsabilidad de Seguros de Salud (HIPAA por sus siglas en inglés) aprobada en Estados Unidos en 1996, están diseñadas para proteger toda la información sensible del paciente, el significativo aumento de las infracciones en materia de datos relacionados con la salud deja entrever la deficiencia de dichas leyes.

Por ejemplo, el ataque del programa WannaCry, que ocasionó daños por un valor superior a 4 mil millones de dólares a nivel mundial, afectó nueve países de América Latina, y directamente a miles de personas en México, Brasil, Chile, Argentina, Ecuador, República Dominicana, Bolivia, Colombia y Venezuela.

La llegada de Internet y el amplio uso de aplicaciones de software administrativo y colaborativo han posibilitado que redes que solían ser circuitos cerrados dentro de los sistemas de los hospitales queden expuestas a amenazas externas. Los equipos de tecnologías de la información tradicionales, así como las medidas de seguridad anticuadas, tales como el uso de contraseñas, los protocolos de encriptación y otras capacidades, se enfrentan ahora a nuevas amenazas que no son capaces de manejar.

Aproximadamente 10 millones de individuos experimentaron un ataque cibernético en 2014, y en la actualidad la cifra es aún mayor.[1]

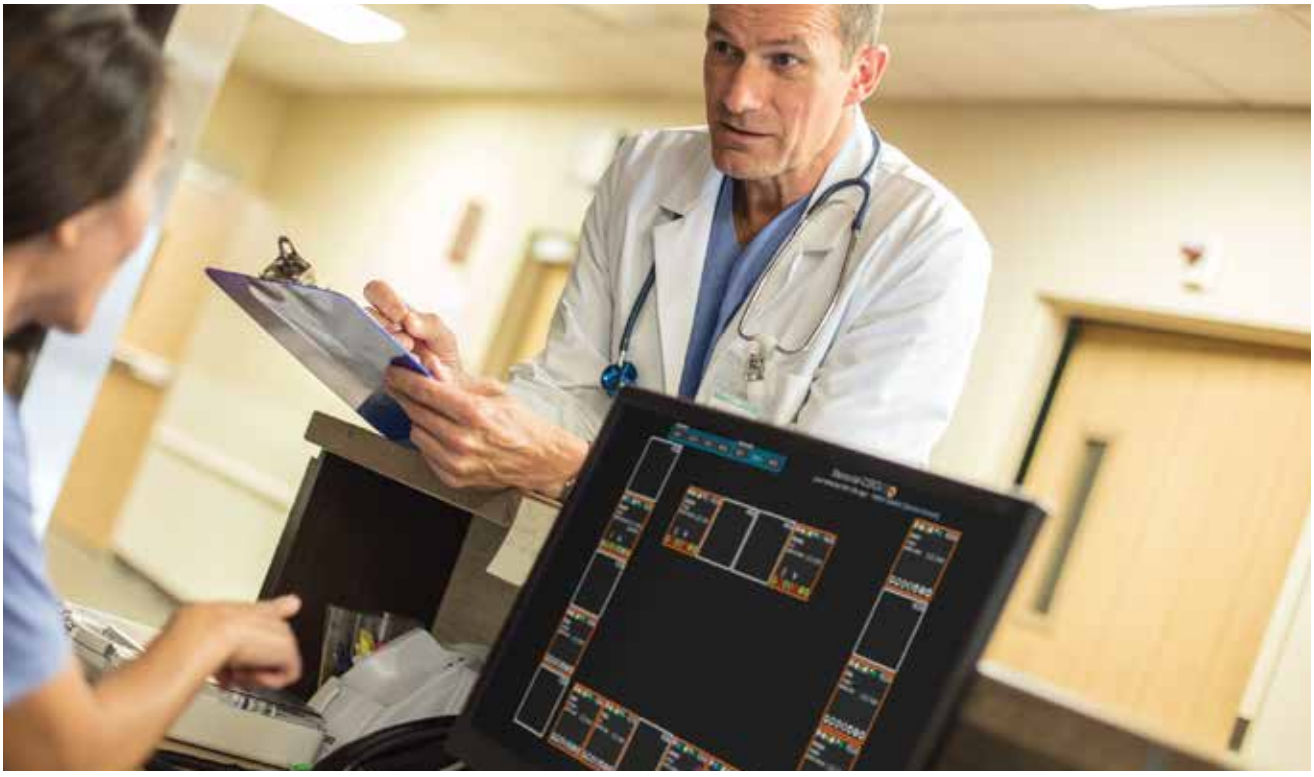


Brasil y México son los países que sufren la mayor cantidad de ataques cibernéticos al año, en América Latina, y las cifras van en aumento.

Entre 2013 y 2014 el crecimiento en los ataques fue del

40%

causando pérdidas anuales por valores superiores a los 93 mil millones de dólares[2]



Motivos por los que se realizan ciberataques a los datos de salud

Durante 2016, fueron sustraídos 2 mil millones de datos personales en EEUU, 100 millones de los cuales eran registros de salud. Las cifras son aún mayores en 2017 y 2018[1]. En América Latina, Brasil y México son los países que sufren la mayor cantidad de ataques cibernéticos al año, con un crecimiento del 40 por ciento en la cantidad de ataques entre 2013 y 2014.

Aproximadamente 10 millones de individuos experimentaron un ataque cibernético en 2014, y en la actualidad la cifra es aún mayor. Además, un estudio sobre delito cibernético realizado por el Registro de Direcciones de Internet para América Latina y el Caribe reveló que los delitos cibernéticos causaron pérdidas anuales por valores superiores a los 93 mil millones de dólares a empresas como bancos y otras organizaciones que dependen en gran medida del uso de Internet para realizar transacciones de negocios.[2]

Pero, ¿qué es lo que está causando esta tendencia tan alarmante? La información contenida en los expedientes de salud es altamente atractiva para el robo de identidad, para hacer fraude con facturas y con las compañías de seguros, y para la extorsión, porque contiene todos los datos sensibles en un solo lugar. La información de tarjetas de crédito y cuentas bancarias tiene una vida útil limitada, ya que la víctima puede cancelar, cambiar o reemplazar las cuentas y tarjetas fácilmente. Sin embargo, los datos de salud no se pueden cambiar tan fácilmente. A esto se suma el hecho de que los datos médicos se pueden monetizar fácilmente y no cambian aun cuando están en peligro.

De igual manera, cuando se trata de información sobre la salud es importante tener en cuenta que está en juego la vida de personas; las organizaciones de salud trabajan en ambientes saturados de aplicaciones, lo que las hace altamente susceptibles a los ataques cibernéticos pues, además, estas organizaciones continúan utilizando sistemas obsoletos. Todos estos hechos hacen que los sistemas de TI de las organizaciones de cuidados en salud no solamente sean vulnerables desde el punto de vista de la seguridad, sino que también sean atractivos como blanco de ataques lucrativos para los delincuentes cibernéticos.

Sin el acceso oportuno a la información requerida, las decisiones clínicas pueden retrasarse y afectar de manera negativa el cuidado del paciente.

La privacidad del paciente y la importancia de la seguridad

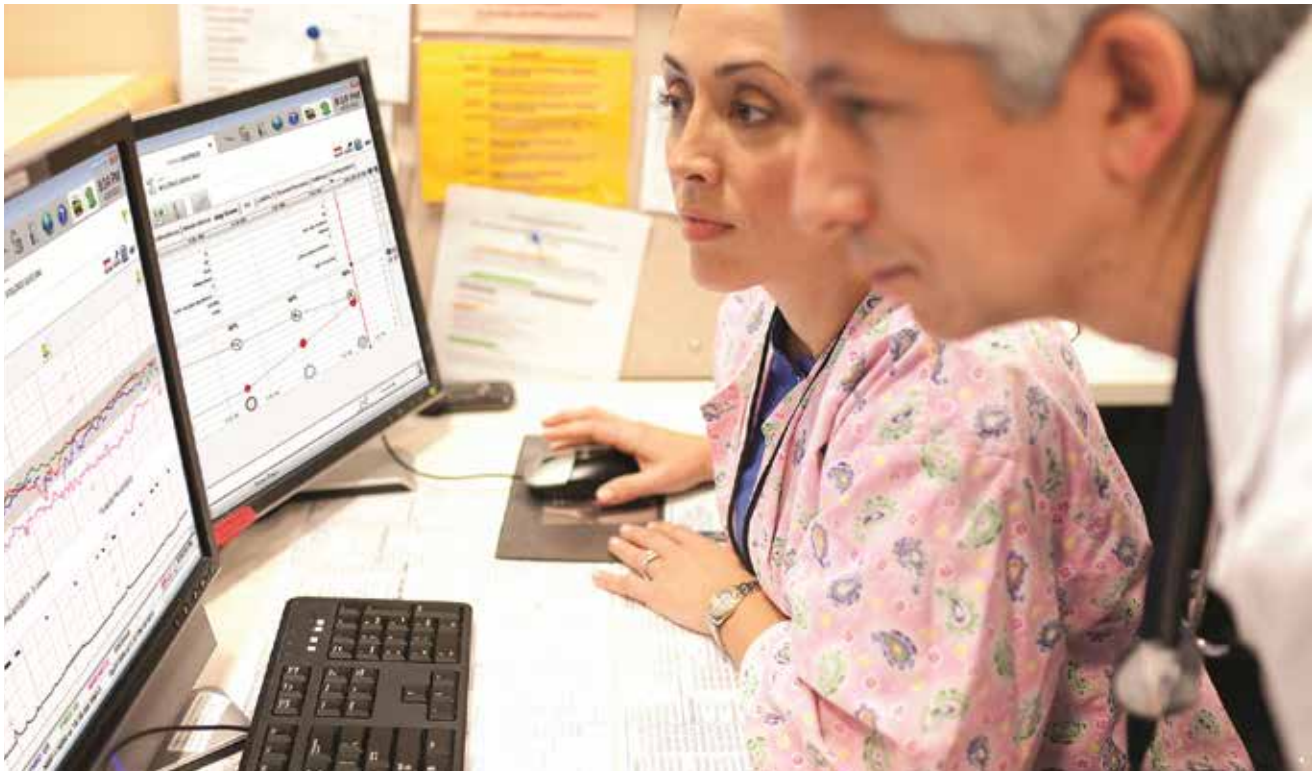
La gestión segura de la información médica electrónica tiene un impacto directo en la calidad de atención al paciente, en sus derechos, en el trabajo de los profesionales de atención en salud y en sus responsabilidades médicas y legales para con los pacientes. Los EMRs permiten a los médicos tomar mejores decisiones para sus pacientes al tener acceso a toda la información de las historias clínicas. Sin el acceso oportuno a la información requerida, las decisiones clínicas pueden retrasarse y afectar de manera negativa el cuidado del paciente.

Cuando la información sobre atención en salud o los sistemas de TI están comprometidos no solamente se generan pérdidas económicas, sino que también puede haber graves consecuencias en forma de pérdidas de vidas, daños irreparables a los prestadores y las empresas de servicios de atención médica, y a todos aquellos asociados con la infracción o el acceso ilegal a los datos.

Impulsar la adopción de portales para la atención en salud

Gracias a los beneficios que ofrecen, los portales de atención en salud y los EMRs se vuelven cada vez más frecuentes. Los sistemas de información actuales deben permitir acceso instantáneo y permanente, facilitar la captura y la obtención de datos y proporcionar funciones de verificación, autentificación, prescripción, seguridad y de reporte en los diferentes departamentos (médico, administrativo y financiero) de manera fácil, accesible y segura.

De igual forma, la implementación de plataformas integrales se hace cada vez más necesaria para garantizar que los datos del paciente se manejen de forma adecuada y para minimizar los riesgos de lesiones, los errores médicos, las reacciones adversas, las complicaciones y todo tipo de resultados no deseables. La adopción y el desarrollo de la nueva generación de sistemas de información son esenciales para seguir siendo competitivos en un entorno de atención en salud basada en la calidad.



Presentamos a Tasy

Philips se compromete a abordar de manera proactiva las inquietudes de seguridad y privacidad de sus clientes. Para lograrlo, ha desarrollado una solución innovadora que permite a los administradores de hospitales acceso integrado a información que puede mejorar la eficiencia de los servicios administrativos. El sistema tiene más de 72 módulos disponibles, siendo uno de ellos el de EMR.

Esta solución puede representar ahorros importantes en costos, dependiendo del caso.

Tasy, diseñado para permitir el acceso rápido e inmediato a la información del paciente, ofrece los siguientes beneficios a las organizaciones y a los profesionales de la salud:

• Solamente utiliza datos seguros, confiables y rastreables.
• Ofrece presupuestos transparentes y mejora la integración, el control y la optimización de las operaciones del hospital.
• Brinda un impacto financiero positivo. Después de implementar Tasy, dos organizaciones de atención médica distintas reportaron incrementos de 50 por ciento en sus ganancias, una reducción de costos del 20 por ciento, reducciones de inventarios del 22 por ciento y reducciones en los retrasos de egresos/altas del 31 por ciento.

El uso generalizado y creciente de Tasy en toda Latinoamérica ha demostrado importantes resultados y un impacto positivo en la vida diaria de miles de pacientes.

Para obtener más información sobre cómo Philips y Tasy pueden ayudarle a mejorar la seguridad y la eficiencia de sus sistemas de TI en la atención de salud, visite el siguiente enlace Philips Tasy: https://www.philips.com.mx/healthcare/resources/landing/tasy

FUENTES
[1] www.checkmarx.com/2018/02/01/january-2018-hacks-breaches/
[2] www.coha.org/cyber-security-and-hacktivism-in-latin-america-past-and-future/