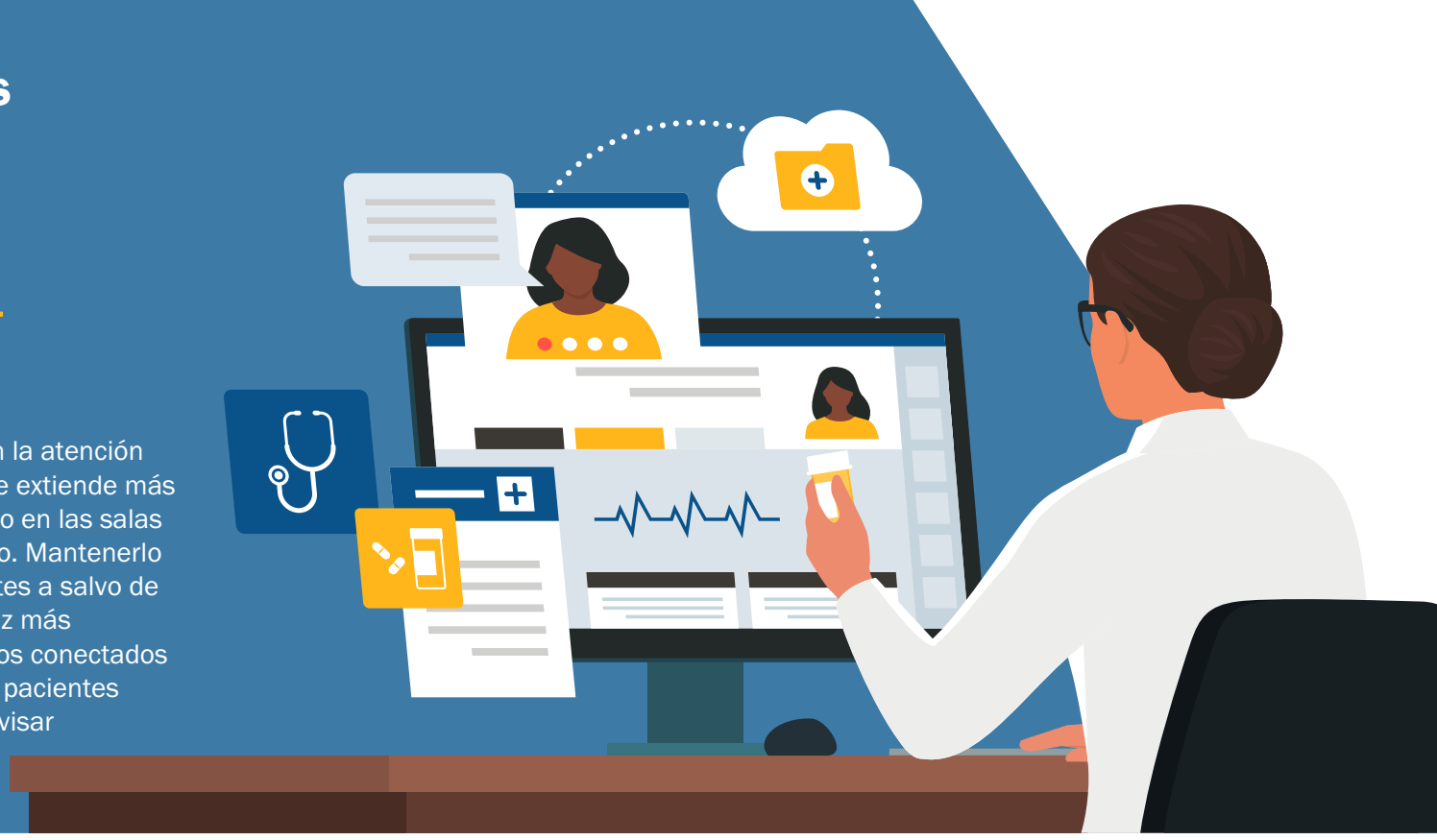
Profesionales Médicos

Cuidar la Ciberseguridad es Cuidar al Paciente

Usted desempeña un papel fundamental en la atención y la seguridad del paciente. Y esa función se extiende más allá de la cama del paciente en un hospital o en las salas de revisión médica en su consultorio médico. Mantenerlo a usted y, en última instancia, a sus pacientes a salvo de las amenazas de ciberseguridad es cada vez más importante. Hoy, con los dispositivos médicos conectados a la red en nuestras instalaciones y que los pacientes utilizan todos los días, es el momento de revisar su "cibergráfico" para detectar signos de advertencia importantes.



Usted evalúa a los pacientes todos los días como parte del desempeño de su trabajo. Pero, ¿hasta qué punto es bueno para evaluar un problema de ciberseguridad cuando se enfrenta a uno?

Cuáles son los riesgos cibernéticos asociados con las siguientes preguntas:

- ¿Cuántos dispositivos médicos conectados a la red utiliza a diario? ¿Tiene asociada una única contraseña "administrativa"?
- ¿Cuántos correos electrónicos recibe de sitios desconocidos pidiéndole que haga clic en un enlace? ¿Cuál es el peligro?
- ¿Usted actualiza su contraseña cuando se lo solicita su organización? ¿Por qué esto es importante?

Estas tres circunstancias proporcionan oportunidades para ciberataques dentro de su organización y los sistemas de red que gestionan la atención al paciente.

- → Cualquier dispositivo conectado a la red aumenta la vulnerabilidad a los ataques.
- → Los correos electrónicos con enlaces deben abrirse con precaución. Asegúrese de saber quién es el remitente antes de hacer clic en cualquier enlace. La seguridad del paciente podría estar en riesgo debido a una infracción causada por un ataque de *phishing*.
- → Actualice siempre sus contraseñas cuando se le solicite para mantener su red segura y nunca comparta su(s) contraseña(s) con nadie.

Desde dispositivos médicos conectados a la red hasta la gestión de contraseñas, todos estos son pasos de cuidado críticos para preservar su seguridad cibernética y la de su organización. Si alguna de estas situaciones se aplica a usted, póngase en contacto con su administrador o gerente de TI para obtener más información sobre su unidad o departamento específico.

¿Sabe cuál es el dispositivo médico conectado junto a la cama del paciente con las mayores vulnerabilidades? **N.º 1 La bomba de infusión**[1]

El sector de la atención médica sufre más ciberataques que cualquier otro sector, ya que absorbe entre un **100 y un 200 %** más de ataques que el sector más próximo.[1,2]

Gracias al volumen de información de salud protegida (Personal Health Information, PHI) confidencial, los registros médicos pueden alcanzar hasta **50 veces** la cantidad que obtienen las tarjetas de crédito robadas en el mercado negro.[1,2]

1. Fuente: A Cynerio Report: The State of IoMT Device Security 2022
2. Fuente: Verizon Data Breach Report 2022

HHS 405(d)
Aligning Health Care Industry Security Approaches

Para obtener más información sobre cómo puede proteger a sus pacientes de las amenazas cibernéticas, consulte la publicación **Prácticas de ciberseguridad de la industria de la salud: gestión de amenazas y protección de pacientes**. Consulte los recursos disponibles que 405(d) tiene para ofrecer en nuestras páginas de redes sociales: **@ask405d** en **Facebook**, **Twitter**, **LinkedIn** e **Instagram**.

Administradores de Consultas y Profesionales de TI

Cuidar la Ciberseguridad es Cuidar de Forma TOTAL

Estas funciones en las organizaciones de atención médica desempeñan un papel fundamental en mantener a los pacientes, los visitantes y las redes hospitalarias a salvo de las amenazas de ciberseguridad.

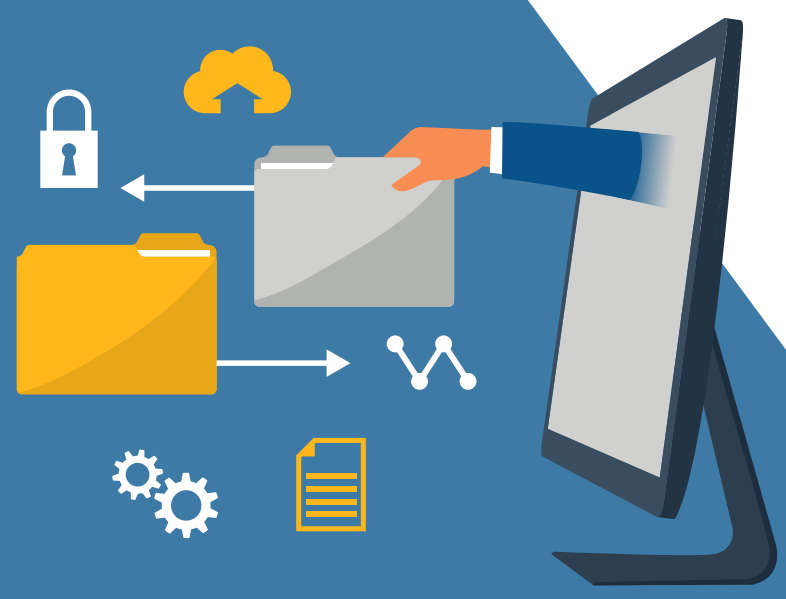
La **gestión de consultas médicas** incluye acceso y registro de pacientes, contabilidad de pacientes, sistemas de programación de pacientes, gestión de reclamaciones y procesamiento de facturas.

Las **operaciones comerciales** incluyen cuentas por pagar, cadena de suministro, recursos humanos, TI, educación del personal, protección de la información del paciente y continuidad del negocio/recuperación de desastres.

La **tecnología de la información de la atención médica** es un componente crítico de casi todas las organizaciones de atención médica. Las aplicaciones de software de gestión empresarial, dispositivos médicos y registros médicos electrónicos (RME) se han integrado en la práctica clínica y las operaciones de la atención médica.

Mejores prácticas de ciberseguridad para proteger los datos de los pacientes:

Desde dispositivos médicos conectados a la red hasta la gestión de contraseñas, todos estos son pasos de cuidado críticos para mantener los registros de atención médica de sus pacientes ciberseguros.



Protección con Contraseña	Actualice su contraseña cuando se le solicite y utilice contraseñas seguras en todas las redes.
MFA (autenticación multifactor)	Utilice el cifrado de toda la información confidencial del paciente.
Cifrado	Instale software de cifrado en cada punto de conexión.
Actualizaciones de Software	Actualice sus programas de software para mantener las actualizaciones de seguridad.

HHS 405(d)
Aligning Health Care Industry Security Approaches

Para obtener más información sobre cómo puede proteger a sus pacientes de las amenazas cibernéticas, consulte la publicación **Prácticas de ciberseguridad de la industria de la salud: gestión de amenazas y protección de pacientes**. Consulte los recursos disponibles que 405(d) tiene para ofrecer en nuestras páginas de redes sociales: **@ask405d** en **Facebook**, **Twitter**, **LinkedIn** e **Instagram**.