CYBER READINESS
INSTITUTE

Prácticas recomendadas sobre ciberseguridad para la telemedicina

El panorama de la atención sanitaria es diferente ahora que hace ocho meses. La telemedicina está más extendida más que nunca y existen nuevas políticas para comprender y aplica en su consulta. A pesar de todos estos cambios, un problema sigue siendo el mismo: hay una cantidad extraordinaria de información de identificación personal, sensible y confidencial integrada en nuestro sistema de atención sanitaria.

Los temas de acceso y seguridad siempre han sido importantes, sobre todo cuando las consultas empezaron su transición a unos registros sanitarios electrónicos. Con la creciente popularidad de la telemedicina, ahora es más importante que nunca asegurarse de que su consulta médica comprenda e implemente comportamientos básicos de higiene cibernética para proteger los datos comerciales y de los pacientes. Crear una cultura de preparación cibernética dentro de su consulta no solo reducirá el riesgo de ser pirateado, sino que también lo preparará y lo equipará mejor con las herramientas adecuadas si sufre un ataque. Basándose en el comportamiento humano e identificando a una persona de contacto, o “responsable cibernético”, dentro de su consulta, el Cyber Readiness Institute lo anima a que se centre en la educación y concienciación como su mejor defensa y oportunidad para la resiliencia.

Los piratas informáticos aprovechan las brechas de seguridad de la telemedicina para lanzar ataques dirigidos a consultas médicas vulnerables. Los investigadores descubrieron que de marzo a abril de este año, las alertas de seguridad enviadas a los departamentos informáticos en 148 hosts de las aplicaciones de telemedicina más populares aumentaron un 30% en general en comparación con el mismo período del año anterior.

A medida que ha aumentado la popularidad de la telemedicina, se ha producido un correspondiente aumento de los ataques dirigidos, incluido un 117% de aumento de las alertas de seguridad solo causadas por las infecciones de malware.

Cuando se trata de temas de telemedicina, tener una base sólida en los conceptos básicos (contraseñas, actualizaciones de software, phishing y uso de dispositivos USB) será muy beneficioso conforme su consulta se adapta al nuevo “entorno de la telemedicina”.

Prácticas recomendadas

Familiarícese con la telemedicina porque ha llegado para quedarse

- Reconozca que la comodidad de la telemedicina la hace atractiva para los pacientes.
- Entienda cómo las emergencias de salud pública declaradas cambian sus protocolos de telemedicina (es decir, reembolso, obtención de licencias interestatales, normativas de la ley HIPAA)

Sea proactivo, no reactivo

- Cree un plan de respuesta ante incidentes, practíquelo y publíquelo entre sus empleados y colegas [Ir a **BeCyberReady.com** para obtener orientación sobre cómo crear un plan de respuesta ante incidentes]

Sea coherente con la plataforma de telemedicina seleccionada durante su consulta

- Entienda qué plataformas de telemedicina son compatibles con la ley HIPAA
- Dé prioridad a sus necesidades y preocupaciones, además de las de sus pacientes, a la hora de valorar las opciones.
- Garantice la uniformidad y transparencia

Infórmese sobre los conceptos básicos de higiene cibernética

- Contraseñas: active la autenticación multifactor y use frases de contraseña con más de 15 caracteres
- Actualizaciones de software: active las actualizaciones automáticas
- Phishing: realice pruebas rutinarias de phishing e informe a sus empleados de cómo son los intentos de phishing
- Dispositivos USB: use el intercambio de archivos en línea en lugar de dispositivos USB

Sea consciente, esté listo y preparado para la cibernética.

Acerca del CRI

El Cyber Readiness Institute es una iniciativa sin fines de lucro que reúne a líderes empresariales de todos los sectores y zonas geográficas para compartir recursos y conocimientos que impulsan el desarrollo de herramientas de seguridad cibernética gratuitas para las pequeñas y medianas empresas (pymes). Explore los elementos básicos de una buena ciberseguridad con nuestro kit básico o cree una cultura de preparación cibernética en su organización con el Programa de Preparación Cibernética autodirigido y disponible en línea. Nuestras guías sobre Recursos de trabajo remoto y Lugar de trabajo híbrido ofrecen consejos oportunos para abordar los cambiantes retos cibernéticos de hoy en día. Para obtener más información, visite www.BeCyberReady.com.