Saint Anthony Hospital está emitiendo un aviso sobre un evento reciente de seguridad de datos, que aún está bajo investigación y puede afectar la información de ciertos pacientes. Mientras continuamos investigando y trabajando para notificar directamente a los pacientes afectados, le brindamos información sobre el evento, nuestra respuesta y los pasos que puede tomar para protegerse contra la posibilidad de robo de identidad y fraude.

¿Qué pasó? El 18 de diciembre de 2023, Saint Anthony tuvo conocimiento de una actividad sospechosa dentro de nuestra red informática. Tomamos medidas inmediatas para proteger la red, garantizar que la atención al paciente no se viera interrumpida e investigamos para determinar la naturaleza y el alcance de la actividad con la ayuda de especialistas en ciberseguridad líderes en la industria. El 7 de enero de 2024, la investigación determinó que los archivos que contenían información de algunos pacientes habían sido copiados de la red por un actor desconocido el 18 de diciembre de 2023.

Como resultado, Saint Anthony llevó a cabo una revisión larga y exhaustiva de los archivos involucrados para identificar y notificar a los pacientes potencialmente afectados, lo cual aún está en curso en este momento. Aunque se desconocen los tipos específicos de información afectada, no ha habido indicios de que la base de datos de registros médicos electrónicos (EMR) del hospital o los sistemas financieros en su conjunto estuvieran comprometidos. Una vez que se complete esta revisión, continuaremos trabajando lo más rápido posible para enviar una carta de notificación directamente a los pacientes potencialmente afectados, que incluirá acceso a servicios gratuitos de monitoreo de crédito y protección de identidad.

¿Qué pacientes/qué información se vieron afectados? La revisión de Saint Anthony aún está en curso para determinar qué pacientes y qué tipos de información se vieron potencialmente afectados por este incidente. Una vez que sepamos más, proporcionaremos información actualizada y enviaremos cartas de notificación por correo a los pacientes potencialmente afectados.

Qué estamos haciendo. Las principales prioridades de Saint Anthony son la ciberseguridad y la privacidad de la información de los pacientes a su cargo. Nuestra rápida respuesta a este evento nos permitió continuar brindando atención al paciente sin interrupción. Como parte del compromiso continuo de Saint Anthony con la privacidad de los datos, estamos trabajando para revisar las políticas y procedimientos existentes e implementar otros adicionales según sea necesario. Saint Anthony informó de inmediato este incidente al FBI y está cooperando con su investigación. También informamos de este incidente a los reguladores correspondientes, incluido el Departamento de Salud y Servicios Humanos de EE. UU.

Qué pueden hacer las personas afectadas. Si bien todavía estamos trabajando para determinar la cantidad de pacientes de Saint Anthony involucrados, se alienta a los pacientes potencialmente afectados a permanecer atentos a los incidentes de robo de identidad. Revise sus estados de cuenta y explicaciones de beneficios para detectar actividades inusuales y reportar cualquier actividad sospechosa de inmediato a su compañía de seguros, proveedor de atención médica o institución financiera. Puede encontrar detalles adicionales a continuación en los *Pasos que puede seguir para ayudar a proteger su información.*

Para más información. Si tiene preguntas adicionales, llame a la línea de asistencia exclusiva que hemos establecido en 888-368-7518, de lunes a viernes, de 8 a.m. y 8 p.m. Tiempo central. O para hablar con alguien directamente del Hospital Saint Anthony, puede llamar al 1-888-211-6763.

Pasos que puede seguir para ayudar a proteger su información

Monitorea tus cuentas

Según la ley estadounidense, un consumidor tiene derecho a un informe crediticio gratuito al año de cada una de las tres principales agencias de informes crediticios: Equifax, Experian y TransUnion. Para solicitar su informe de crédito gratuito, visite www.annualcreditreport.com o llame gratis al 1-877-322-8228. También puede comunicarse directamente con las tres principales agencias de informes crediticios que se enumeran a continuación para solicitar una copia gratuita de su informe crediticio.

Los consumidores tienen derecho a colocar una "alerta de fraude" inicial o extendida en un expediente de crédito sin costo alguno. Una alerta de fraude inicial es una alerta de un año que se coloca en el expediente crediticio de un consumidor. Al ver una alerta de fraude en el expediente crediticio de un consumidor, una empresa debe tomar medidas para verificar la identidad del consumidor antes de otorgarle un nuevo crédito. Si es víctima de robo de identidad, tiene derecho a una alerta de fraude extendida, que es una alerta de fraude que dura siete años. Si desea colocar una alerta de fraude, comuníquese con cualquiera de las tres principales agencias de informes crediticios que se enumeran a continuación.

Como alternativa a una alerta de fraude, los consumidores tienen derecho a colocar un "congelamiento de crédito" en un informe crediticio, lo que prohibirá a una agencia de crédito divulgar información en el informe crediticio sin la autorización expresa del consumidor. El congelamiento de crédito está diseñado para evitar que se aprueben créditos, préstamos y servicios a su nombre sin su consentimiento. Sin embargo, debe tener en cuenta que utilizar un congelamiento de crédito para controlar quién tiene acceso a la información personal y financiera en su informe de crédito puede retrasar, interferir con, o prohibir la aprobación oportuna de cualquier solicitud o solicitud posterior que realice con respecto a un nuevo préstamo, crédito, hipoteca o cualquier otra cuenta que implique la extensión de crédito. De conformidad con la ley federal, no se le puede cobrar por colocar o levantar un congelamiento de crédito en su informe crediticio. Para solicitar un congelamiento de seguridad, deberá proporcionar la siguiente información:

1. Nombre completo (incluyendo la inicial del segundo nombre, así como Jr., Sr., II, III, etc.);
2. Número de Seguro Social;
3. Fecha de nacimiento;
4. Direcciones de los dos a cinco años anteriores;
5. Comprobante de dirección actual, como una factura de servicios públicos o de teléfono actual;
6. Una fotocopia legible de una tarjeta de identificación emitida por el gobierno (licencia de conducir estatal o tarjeta de identificación, identificación militar, etc.); y
7. Una copia del informe policial, informe de investigación o denuncia ante una agencia policial sobre robo de identidad si es víctima de robo de identidad.

Si desea colocar una alerta de fraude o un congelamiento de crédito, comuníquese con las tres principales agencias de informes crediticios que se enumeran a continuación:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert,P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Información adicional

Puede obtener más información sobre el robo de identidad, las alertas de fraude, la congelación de crédito y los pasos que puede seguir para proteger su información personal comunicándose con las oficinas de informes del consumidor, la Comisión Federal de Comercio o el Fiscal General de su estado. Puede comunicarse con la Comisión Federal de Comercio en: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.robodeidentidad.gov; 1-877-ROBO DE IDENTIDAD (1-877-438-4338); y TTY: 1-866-653-4261. La Comisión Federal de Comercio también alienta a quienes descubran que su información ha sido utilizada indebidamente a presentar una queja ante ellos. Puede obtener más información sobre cómo presentar dicha queja a través de la información de contacto indicada anteriormente. Tiene derecho a presentar una denuncia policial si alguna vez sufre un robo de identidad o un fraude. Tenga en cuenta que para presentar una denuncia ante las autoridades por robo de identidad, es probable que deba proporcionar alguna prueba de que ha sido víctima. Los casos de robo de identidad conocido o sospechado también deben informarse a las autoridades y al Fiscal General de su estado. Este aviso no ha sido demorado por las autoridades.