Lo que necesita saber sobre la pérdida de datos con información privilegiada accidental o maliciosa:

"Una amenaza interna en la industria de la atención médica es potencialmente una persona dentro de una organización de atención médica, o un contratista, que tiene acceso a activos o información interna sobre las prácticas de seguridad, los datos y los sistemas informáticos de la organización".
—Departamento de Salud y Servicios Humanos

Recuerde que las amenazas internas son un riesgo grave. Pueden implicar a personas de su organización que tengan acceso legítimo a sus sistemas informáticos y a su red. Podría ser un simple error humano, negligencia o malicia lo que hace que personas dentro de la organización comprometan los datos de sus pacientes y de su empresa.

Pasos a seguir

Revise esta lista de mejores prácticas y pasos a seguir para preservar su seguridad y la de su organización.

Acción: informar

Póngase en contacto con su administrador de TI, gerente de la clínica o supervisor inmediato.

Es imprescindible que la acción sea rápida. ¡Esta amenaza es real!

Seis razones para proteger los datos de atención médica

1. Transmisión de datos confidenciales: información de identificación personal/ información de salud protegida
2. Los datos confidenciales comprenden la mayoría de sus tareas diarias.
3. La información de salud protegida se analiza, procesa y transmite diariamente entre los sistemas de información.
4. Proteger los datos confidenciales requiere políticas, procesos y tecnologías sólidos.
5. Los impactos en su organización pueden ser profundos si los datos se corrompen, pierden o roban.
6. Las infracciones de seguridad pueden impedir que los usuarios completen su trabajo a tiempo y podrían afectar negativamente a la atención al paciente.

HHS 405(d)
Knowledge on Demand

¡Si lo ve, dígalo!

- ☑ **Las medidas proactivas contribuyen mucho** a protegerlo a usted y a los datos que gestiona.
- ☑ **Siga su instinto** y siempre informe lo que no luzca bien o le resulte inadecuado.
- ☑ **Póngase siempre en contacto con su gerente o administrador de TI** si cree que puede ser víctima de una pérdida de datos o si cometió un error sin intención. La rapidez es clave.
- ☑ **Cada situación variará.** Su gerente o los profesionales de seguridad de TI podrán guiarle mejor, ya que las amenazas cibernéticas no se limitan a solo al hackeo.

Informar

Informar a:

Información de contacto:

Para obtener más recursos e información sobre cómo puede proteger a sus pacientes de las amenazas cibernéticas, consulte la publicación *Prácticas de ciberseguridad de la industria de la salud (Health Industry Cybersecurity Practices, HICP): gestión de amenazas y protección de pacientes* en 405d.hhs.gov.