1129 20th Street, NW
Suite 400
Washington, DC 20036

T. 202 466.8960
F. 202. 293.8103
www.ftlf.com

MEMORÁNDUM

PARA: Gina Capra
Vicepresidenta, Capacitación y Asistencia Técnica
Asociación Nacional de Centros de Salud Comunitarios (NACHC)

DE: Dianne Pledgie, Socia
Amanda Pervine, Asociada

FECHA: 25 de abril de 2020

ASUNTO: Cumplimiento de HIPAA y teletrabajo

Este memorándum responde a un pedido de información sobre el cumplimiento de HIPAA para los empleados de centros de salud en el entorno del teletrabajo. Específicamente, usted solicitó respuestas a las siguientes preguntas:

I. ¿Qué se requiere para garantizar que un empleado mantenga el cumplimiento de HIPAA en su ambiente remoto o de teletrabajo?

Donde sea que trabaje un empleado del centro de salud - en una clínica, en el hogar de un paciente, en una feria de salud, en la oficina administrativa o en el hogar - las Normas de HIPAA se aplican a la información de salud protegida ("PHI", por sus siglas en inglés) de los pacientes. Con el reciente y rápido cambio al teletrabajo, los centros de salud deben identificar riesgos de cumplimiento adicionales de HIPAA e implementar estrategias para mitigar esos riesgos. A continuación se describen algunos requisitos de cumplimiento relevantes en virtud de las Normas de Privacidad y Seguridad de HIPAA, junto con consideraciones para los centros de salud y el teletrabajo.

En virtud de los requisitos administrativos de la Norma de Privacidad de HIPAA, las entidades cubiertas deben (entre otras cosas) desarrollar e implementar políticas y procedimientos escritos, capacitar a los miembros de la fuerza laboral, y mantener salvaguardias razonables y apropiadas. Con el teletrabajo, los centros de salud deben considerar:

- Políticas y procedimientos: Si su centro de salud tiene una política de teletrabajo separada que está enfocada de manera estrecha (es decir, sólo se aplica a los proveedores o administradores de casos), determine si se puede ampliar para cubrir toda la fuerza laboral remota (es decir, facturación, codificación, calidad, gestión de riesgos). Los centros de salud que no tienen una política de teletrabajo pueden desarrollar una o revisar/repasar sus políticas de HIPAA para aplicarlas al entorno de teletrabajo. Los centros de salud deben proporcionar políticas nuevas o revisadas para todos los empleados afectados.
- Capacitación: Si su centro de salud adopta políticas nuevas o revisadas, brinde capacitación a los empleados afectados sobre las políticas y conserve la documentación relacionada (diapositivas, registros de asistencia, etc.). Los centros de salud deben revisar y modificar los módulos de

capacitación anual y de los nuevos empleados de HIPAA para reflejar el entorno de teletrabajo.

- Salvaguardias: Las salvaguardias administrativas, técnicas y físicas de su centro de salud deben ser revisadas para responder a los riesgos para PHI en el entorno del teletrabajo. Por ejemplo, ¿cómo deben los empleados manejar los documentos que contienen PHI? Considere si se pueden limitar los privilegios de impresión, cómo los empleados deben proteger los documentos, y si los empleados pueden destruir los documentos usando una trituradora.

En virtud de la Norma de Seguridad de HIPAA, las entidades cubiertas deben mantener salvaguardias administrativas, técnicas y físicas razonables y adecuadas para proteger la PHI electrónica ("ePHI"). En primer lugar, los centros de salud deben identificar los posibles riesgos y vulnerabilidades de la e-PHI en el entorno del teletrabajo. El análisis de riesgos permite a cada centro de salud desarrollar estrategias apropiadas para mitigar sus riesgos específicos. A los centros de salud les puede resultar útil agrupar su uso en el marco descrito en la guía de la Oficina de Derechos Civiles sobre el uso y el acceso a distancia[1]:

- Acceso: Determinar qué empleados requieren acceso a la ePHI y cómo lo harán. Considere los dispositivos utilizados (dispositivos emitidos por el centro de salud o dispositivos personales), así como el acceso al sistema (autenticación).
- Almacenamiento: Determine si se permitirá a los empleados almacenar la ePHI y, en caso afirmativo, cómo se protegerá. Si bien un centro de salud puede prohibir la descarga y el almacenamiento de ePHI a través de la configuración de los dispositivos emitidos por el centro de salud, se requerirán otras estrategias para los empleados que utilicen dispositivos personales para el teletrabajo.
- Transmisión: Determinar cómo los empleados transmitirán ePHI. Los centros de salud pueden requerir que los empleados accedan al correo electrónico, a los registros médicos y a otros sistemas que contengan ePHI a través de una red segura.

2. ¿Cuál es el texto de certificación de muestra y/o un enfoque recomendado para los gerentes?

Muchas entidades cubiertas requieren que los empleados firmen un acuerdo de confidencialidad que detalla las responsabilidades de cumplimiento de HIPAA del empleado. Como punto de partida, los centros de salud deben revisar el acuerdo de confidencialidad de sus empleados. Si éste aborda adecuadamente el cumplimiento de las políticas de HIPAA del centro de salud en el entorno del teletrabajo, el centro de salud puede recordar a los empleados los requisitos de cumplimiento del acuerdo de confidencialidad.

---

[1] Disponible en: https:// / w w w.hhs .g o v / sit es/ d efault / fi les/ocr /privacy/hipaa/administ rat ive/ secu rityru le/remot euse.p d f?lang uag e=es.

Si el acuerdo de confidencialidad está redactado de forma restrictiva, o el centro de salud determina que el teletrabajo debe ser mencionado específicamente, debe revisarse el acuerdo de confidencialidad. Los centros de salud también deben revisar su política para documentar que los empleados han recibido, entienden y están de acuerdo en cumplir con las políticas nuevas o revisadas de HIPAA. Por ejemplo, si un centro de salud implementa una nueva política de teletrabajo, los empleados podrían dar fe de que la han recibido y que están de acuerdo en cumplirla firmando la política o un formulario de certificación.

Además de recordar a los empleados sus continuas responsabilidades de cumplimiento, los gerentes deben continuar controlando el cumplimiento de los empleados respecto de las políticas y los procedimientos aplicables de HIPAA. Los gerentes deben recordar a los empleados su deber de reportar cualquier pregunta, preocupación o posible incumplimiento a sus gerentes y/o a los Oficiales de Privacidad y Seguridad de HIPAA.