News
New Jersey
Office of the Attorney General
NEW JERSEY DEPARTMENT OF LAW & PUBLIC SAFETY

Christopher S. Porrino
Fiscal General

División de Asuntos del Consumidor
Steve C. Lee, *Director*

División de Leyes
Michelle Miller, *Directora Interina*

Para publicación inmediata:
Día 17 de Febrero del 2017

Para más información contacte:
Lisa Coryell 973-504-6327
C. John Schoonejongen 973-504-6327

Horizon Blue Cross/Blue Shield de Nueva Jersey acuerda a pagar $1.1 millones, reforzar la seguridad de datos, para resolver las alegaciones de lapsos de seguridad en la información personal de los asegurados

NEWARK –La New Jersey Division of Consumer Affairs hoy anunció que el más grande proveedor de seguro de salud del estado, Horizon Healthcare Services, Inc., ha acordado a pagar $1.1 millones y mejorar las prácticas de seguridad de los datos para resolver alegaciones que no protegió la privacidad de casi 690,000 asegurados de New Jersey cuya información personal estaba contenida en dos computadoras portátiles robadas de la oficina principal en Newark.

La aseguradora gigante, la cual hace negocios como Horizon Blue Cross Blue Shield de New Jersey ("Horizon BCBSNJ"), dio su consentimiento al acuerdo después de que la investigación de la División concluyó que el incumplimiento de los estándares de seguridad federales de la compañía era un peligro que exponía la información personal de sus miembros – incluyendo sus nombres, direcciones fecha de nacimiento, identificación de seguro y en algunos casos Números de Seguro Social y datos clínicos limitados. El Estado alega que la información de los asegurados en las computadoras portátiles, aunque la contraseña estaba protegida, no estaba encriptada, como es requerido bajo estas circunstancias por el acta federal Health Insurance Portability Accountability Act, enmendado por el Health Information Technology for Economic and Clinical Health Act ("HIPAA/HITECH").

"Proteger la información personal de los asegurados debe ser una de las prioridades de cada compañía. Los consumidores se lo merecen y la ley lo demanda," dijo Steve Lee, Director de la Division of Consumer Affairs. "Los alegados lapsos de Horizon Blue Cross Blue Shield of New Jersey arriesgaron exponer la información personal más privada de los asegurados al público, dejándolos muy vulnerables al robo de identidad. Este acuerdo asegura que Horizon BCBSNJ mantendrá los apropiados protocolos de seguridad de privacidad de los datos para prevenir futuras brechas de seguridad."

Las computadoras portátiles fueron robadas de la oficina principal de Horizon BCBSNJ's Newark en Noviembre del 2013 cuando alguien cortó los cables que las aseguraban a un escritorio. La investigación de la División reveló que durante el fin de semana del robo, personal de los proveedores externos preformó renovaciones y servicios de mudanzas y tuvo acceso sin supervisión a las áreas donde las computadoras fueron robadas. Las computadoras contenían Electronic Protected Health Information o "ePHI," lo cual está protegido bajo HIPAA/HITECH.

Después de un incidente en el que una Horizon BCBSNJ computadora portátil fue robada del maletero de un auto de un empleado en Enero del 2008, Horizon BCBSNJ cambió su política de corporación y requirió que todas las computadoras portátiles de la compañía tuvieran software encripta. En Mayo del 2008, Horizon BCBSNJ hizo una declaración pública de que la compañía había completado encriptación en todas las computadoras de escritorios y portátiles, así como sus aparatos móviles, y los empleados de la compañía habían sido entrenados en encriptación para que hubiera completo entendimiento de las nuevas medidas de seguridad que fueron adoptadas después del incidente.

Sin embargo, la investigación de la División concluyó que más de 100 computadoras portátiles asignadas a empleados no estaban encriptadas. La mayoría de las computadoras sin encriptación habían sido obtenidas fuera de lo procedimientos normales, y por lo tanto no detectadas por el departamento IT de corporación de Horizon BCBSNJ, según la investigación. Como tal, la investigación descubrió que el departamento IT no monitoreó adecuadamente, el servicio, o instaló software de seguridad requerida de la política de corporación de esas computadoras. La investigación además reveló que las computadoras portátiles robadas en el 2013 fueron dadas a empleados que no estaban requeridos guardar un ePHI en sus computadoras portátiles, en violación de una póliza de la compañía limitando acceso a ePHI información a empleados que la necesitaban para completar sus funciones de trabajo.

El Estado alega que Horizon BCBSNJ se involucró en múltiples violaciones del New Jersey Consumer Fraud Act, el federal HIPAA/HITECH y sus Privacy and Security Rules por acciones que incluyen:

- No implementar los procedimientos para la autorización y o supervisión de los empleados que trabajaron con ePHI o en lugares donde se podía tener acceso a éste.
- No identificar y responder a sospechados incidentes de seguridad; mitigar, a un punto factible los efectos de incidentes de seguridad que se conocían; y documentar incidentes de seguridad y los resultados.
- No implementar una periódica evaluación técnica y no técnica en respuesta a los cambios ambientales o cambios operacionales que afectaban la seguridad del ePHI que establecía la medida a la que sus políticas de seguridad y procedimientos satisfacían los requisitos bajo la HIPAA's Security Rule.
- No implementar las políticas y procedimientos para proteger su facilidad y el equipo en ésta de acceso físico no autorizado, manipulación y robo.
- No mantener un archivo de la movilidad de la media de hardware y electrónica contenida en ePHI y de cualquiera persona responsable.
- No implementar un mecanismo para encriptar y de encriptar ePHI.
- No adecuadamente entrenar a todos los miembros de su trabajo en las políticas y procedimientos con respecto a la Protected Health Information, o "PHI," el cual está sujeto a las reglas de HIPAA.
- No proteger razonablemente PHI del uso intencionado o sin intención o declaración de que es una violación de los estándares, especificaciones de implementación, o de otros requisitos bajo la HIPAA's Privacy Rule.
- Diciendo que había implementado y estaba manteniendo apropiadas medidas de seguridad para proteger la información de los miembros bajo HIPAA, y de que había apropiadamente entrenado a los empleados en esas medidas, cuando eso no era el caso.
- Después del incidente del 2008, diciendo que Horizon BCBSNJ tomaría adicionales medidas para prevenir futuros robos de computadoras portátiles, cuando tales medidas no se habían tomado o eran inefectivas.

Bajo el acuerdo, Horizon BCBSNJ tiene que implementar un Plan de Acción Correctivo (Corrective Action Plan) que incluya emplear a una parte tercera profesional para conducir un análisis minucioso de riesgo de seguridad asociado con el almacenamiento, transmisión y recibo de ePHI, y de remitir un reporte de esos descubrimientos a la División dentro de los 180 días del acuerdo y cada año después por dos años. Horizon BCBSNJ también acordó a pagar un $1.1 millón de dinero compuesto de $926,803.22 de multa civil, $93,196.78 reembolso a Estado de costos de abogados y de investigación, y $80,000 para ser usado a la sola discreción del Attorney General para la promoción de programas de privacidad y para la implementación de iniciativas de privacidad para el consumidor. Bajo el acuerdo, $150,000 en multas civiles serán suspendidas pendiendo Horizon BCBSNJ's cumplimiento con la Final Consent Judgment.

El Investigator Brian Morgenstern de la Division of Consumer Affairs' Cyber Fraud Unit condujo la investigación.

Los Deputy Attorneys General Elliott M. Siebers y Russell M. Smith, Jr., y los Assistant Attorneys General John M. Falzone III y Brian McDonough, representaron al Estado de New Jersey en este asunto.

Jeffrey S. Chiesa of Chiesa Shahinian & Giantomasi, P.C., y Theodore J. Kobus III y Eric Packel of BakerHostetler, representaron a los acusados en este caso.

Consumidores que creen han sido engañados o estafados por negocio o sospechan cualquier otro abuso de consumo, pueden poner una queja en línea con la State Division of Consumer Affairs yendo al sitio web de ésta o llamando al 1-800-242-5846 (gratis si llama desde New Jersey) o al 973-504- 6200.

Siga la New Jersey Attorney General's Office en línea en Twitter, Facebook, Instagram & YouTube. Los enlaces a los medios sociales proveídos son por referencias solamente. La New Jersey Attorney General's Office no apoya o patrocina ningún sitio web, compañías o aplicaciones que no sean del gobierno.