SANDBERG PHOENIX

LONG TERM CARE & SENIOR LIVING BLOG

Triple-S to Pay $3.5 Million Plus Adopt a Robust Corrective Action Plan

AUTHOR: SANDBERG PHOENIX

Office of Civil Rights (OCR) Director Jocelyn Samuels has made it clear that the "OCR remains committed to strong enforcement of the HIPAA Rules." The latest settlement announced on 11/30/15 concerning Triple-S, an insurance holding company offering a wide range of insurance products and services, demonstrates just how committed the OCR is when it comes to HIPAA compliance. This settlement included payment of $3.5 Million and adopting a corrective action plan to implement a robust and comprehensive HIPAA compliance program pursuant to the Resolution Agreement entered by Triple-S.

Here's what went wrong – this OCR settlement resulted following an OCR investigation initiated after Triple-S reported multiple breach notifications to the OCR. The investigation revealed "widespread non-compliance" with HIPAA including:

- Failure to implement appropriate administrative, physical, and technical safeguards to protect PHI;
- Impermissible disclosures of PHI to an outside vendor that did not have an appropriate Business Associate Agreement with Triple-S;
- Use or disclosure of more PHI that was necessary to carry out mailings;
- Failing to conduct an accurate and through risk analysis incorporating all IT equipment, applications and data systems using ePHI; and
- Failing to implement security measures sufficient to reduce risks and vulnerabilities to ePHI to a reasonable and appropriate level.

As noted above, here's what the OCR required from Triple-S to settle the potential violations – payment of $3.5 Million plus entering into a Plan of Correction to implement a comprehensive HIPAA compliance program. Here's what the comprehensive compliance program will include to protect the security, confidentiality, and integrity of the PHI Triple-S collects from its beneficiaries:

- Risk analysis and a risk management plan;

- Procedure to evaluate and address any environmental or operational changes that affect the security of the ePHI the company holds;
- Policies and procedures to ensure compliance with HIPAA Rule requirements;
- Training program covering Privacy, Security and Breach Notification Rules requirements, for all workforce members and business associate providing services at Triple-S premises.

The OCR has once again clearly demonstrated its commitment to enforcing the HIPAA Rules. In this case, repeated breach notifications brought an OCR investigation to Triple-S. That investigation uncovered potential violations of HIPAA that resulted in this settlement to correct the potential violations the investigation uncovered.

So what's a Covered Entity to do? It's quite simple – be in compliance with HIPAA. Even with the best compliance programs, breaches happen and must be reported to the OCR. The best protection for a Covered Entity undergoing an investigation following the report of a breach is to have a vital HIPAA compliance program already in place. As Triple-S learned, not having a HIPAA compliance program can be costly. In addition to a large payment to the OCR, now Triple-S will have a HIPAA compliance program under the added scrutiny of a Resolution Agreement with the OCR.

In order to avoid the fate of Triple-S, health care providers must bring their HIPAA compliance programs in line with the Privacy and Security Rules. Consult a qualified legal counsel for assistance.

By Denise Bloch

Denise Bloch

Image not found or type unknown