LORICCA
HIPAA COMPLIANCE SPECIALISTS

CASE STUDY

UTAH PRACTITIONER FINED FOR SUPPLIER WITHHOLDING DATA

Relying on Suppliers for business operations has become an essential function for many companies. Do your due diligence and review security controls for suppliers and determine if they meet your security requirements.

ABOUT THE BREACH

March 03, 2020 - The provider office of Steven Porter, MD in Ogden, Utah has settled with the Department of Health and Human Services Office for Civil Rights after failing to implement certain HIPAA security requirements. In addition to the fine, the practitioner must adopt a corrective action plan and is subject to two years of monitoring by OCR.

Porter is the sole practitioner of the medical practice and provides gastroenterological services to more than 3,000 patients each year. His settlement with OCR over potential HIPAA violations is the first announced this year.

OCR launched a compliance review into the practice, after Porter filed a breach report stemming from a business associate dispute. Porter claimed his EHR vendor was impermissibly using the practice's electronic protected health information by blocking the provider's access until he paid the vendor $50,000.

However, the investigation revealed the provider never conducted a security risk assessment (risk analysis) of potential risks and vulnerabilities to the integrity and availability of its ePHI prior to the breach report. The investigation also found the practice did not implement security measures that would sufficiently reduce risks and vulnerabilities to a reasonable level.

ABOUT THE BREACH >>

Further, the practice also allowed its EHR vendor to create, receive, maintain, and transmit ePHI on behalf of the provider since at least 2013, but did not first obtain satisfactory assurances that the vendor would appropriately safeguard the data.[1]

The practice is currently being monitoring by HHS for a period of two years or until the appropriate security controls have been satisfactorily implemented. Additional civil monetary penalties could be imposed for not meeting requirements by the scheduled dates imposed by HHS. [2]

THE LESSONS LEARNED >>

THE LESSONS LEARNED

Failure to implement basic HIPAA requirements, such as having a risk management strategy, to include risk analysis, continues to be a trend within the healthcare industry and can be quite costly. What the Utah Practice experience with HHS should teach organizations today is that Risk Management and Business Associate relations are two vital components for HIPAA Compliance.

Risk management starts with knowing where your data resides and the security controls that are in place to protect the data.

- Conduct a risk assessment annually.
- Review and revise current security management policies and procedures at least annually.

External threats have become more important as companies move towards third parties to manage processes and storage of data.

- Business associate relationships require due diligence on suppliers that store, transmit or access your sensitive data to protect your company and your customers.
- A BAA should be negotiated before any access to sensitive data is provided to the business associate.

HHS has strict guidelines and timeframes for remediation after a breach. Don't delay. For help conducting a Risk Assessment, reviewing your Business Associates/Suppliers, or just to be prepared for an OCR Audit, contact us to learn about our services or click on the links below.

Security Risk Assessments

Supply Chain Risk Management

OCR Audit

FOR HELP PROTECTING YOUR INFRASTRUCTURE AND COMPANY, CONTACT US. www.loricca.com | 855-447-2210

ABOUT LORICCA

Loricca provides the world-class consulting services required to meet today's cybersecurity challenges. Our security professionals bring a wealth of experience with real-life lessons on what works and what doesn't.

We partner with organizations to evaluate, build, and manage their IT Security Programs. Our experience includes extensive healthcare industry, federal state and county governments, media, retail, finance, software, and medical device manufacturing organizations.

Our goal is to keep these organizations and their vendors compliant and protected from the cybersecurity risks of today and tomorrow by delivering high-quality work on time and on budget.

Sources

1. Health IT Security. HIPAA and Compliance News.
2. HHS Resolution Agreement. https://www.hhs.gov/sites/default/files/porter-ra-cap-508.pdf.