

CASE STUDY

HIPAA COMPLIANCE

GAP ASSESSMENT

PENETRATION TESTING



Business Challenges

- Public HIPAA data breach
- Identify compliance gaps with new PCI DSS 3.0 standards
- Internal resources without sufficient time & expertise to quickly remediate issues



Opportunities

- Proactively find gaps in compliance & best practices
- Prioritise remediation steps
- Ongoing consulting & assistance with remediation project planning & implementation



Foresite Solutions

- PCI DSS 3.0 Gap Assessment
- Security & Compliance Advisory Services

BACKGROUND

A hospital group was looking for outside assistance after suffering a very public HIPAA data breach, and subsequently realizing they were not meeting the compliance regulations for PCI DSS 3.0. Foresite's Threat Mitigation Team met with their internal IT groups, and determined that while a recent HIPAA audit had provided them with steps for remediation there was a lack of time for the internal team to oversee the remediation project. The team was concerned the timeline to fix the issues would not be met. Further, it was unclear if the Cardholder Data Environment for PCI compliance had been accurately confirmed after many network changes.

OUR OBJECTIVES



Confirm current scope of PCI Cardholder Data Environment



Provide ongoing support for project management and remediation assistance



Create a Prioritised Approach plan for remediation

OUR RESULTS

A PCI DSS Gap Assessment confirmed the current Cardholder Data Environment and the specific areas where compliance was not being met. This assessment allowed for creation of a prioritized list of items requiring remediation, which could then be assigned to the hospital's various internal teams based on the expertise or systems involved. Through an ongoing Security and Compliance Advisory service with Foresite, the hospital's staff is able to outsource oversight of the projects and have access to resources with specific expertise they don't have a full-time need for but are required for aspects of remediation such as, Payment Card Industry Qualified Security Assessors (PCI

QSA), firewall security specialists, and Healthcare Information Security and Privacy Practitioners (HCISPP). The flexible nature of the Advisory agreement means resources can be both scheduled for specific projects and utilized as needed for:

- HIPAA/PCI Consulting & Remediation
- Penetration testing and vulnerability scans
- Assistance with completing compliance documentation
- 3rd party vendor or solution evaluations
- Outsourced Security Operations Team Incident Response

WORLD HEADQUARTERS

7311 West 132nd Street, Suite 305
Overland Park, KS 66213

+1 800-940-4699

CT OFFICE

1 Hartfield Blvd, Suite 300
East Windsor, CT 06088

info@foresite.com

UK OFFICE

A8 Ively Road, Farnborough
Hampshire, GU14 0LX, UK

+44 800-358-4915