Healthcare providers and payers have the unique challenge of protecting patient privacy and sensitive data, while at the same time increasing access to healthcare services. Fines related to the Health Insurance Portability and Accountability Act (HIPAA) are on the rise, and the US Department of Health and Human Services Office for Civil Rights (OCR) is aggressively and proactively auditing healthcare organizations.

The added risk created by the adoption of complex new technologies from electronic health record (EHR) incentive programs heightens the need for actionable information. With Attack Intelligence from Core Security, Healthcare organizations can:

- Proactively identify potential threats to electronic protected health information (ePHI)
- Focus on the most vulnerable points along attack paths that lead to critical assets such as an EHR database
- Demonstrate risk assessments and prove effective security risk management practices
- Create achievable remediation plans for operations.

**Avoid HIPAA Fines and Protect HITECH Funding**

For healthcare organizations, it is critical to avoid HIPAA fines and protect funding resulting from the Health Information Technology for Economic and Clinical Health (HITECH) Act. According to Meaningful Use regulations, healthcare organizations must meet specific criteria to receive incentive payments offered through the HITECH program. Specifically, Meaningful Use requires that healthcare organizations “protect electronic health information created or maintained by certified EHR technology through the implementation of appropriate technical capabilities”.

To further enforce HIPAA regulations, the OCR is now actively auditing healthcare organizations against a multi-point protocol. Recently, a managed care organization paid $1.7 million to OCR for HIPAA violations, further exhibiting the financial impact of fines. One of the key activities that many healthcare organizations cannot effectively complete is the ability to conduct a risk assessment and implement a risk management program. If these activities cannot be adequately demonstrated, various penalties are enforced including the chance of losing any already acquired Meaningful Use funding.

**Key Benefits**

- Secure critical healthcare assets (ePHI, EHR)
- Improve HIPAA audit readiness and avoid fines
- Maintain incentive payments from HITECH programs
- Lower risk through efficient remediation plans
- Demonstrate effective risk assessments

**Attacks Continue to Rise**

According to the Ponemon Institute’s *Fourth Annual Benchmark Study on Patient Privacy and Data Security*:

- 90% of healthcare organizations have reported a data breach in the past two years.
- Attacks on healthcare systems have increased 100% since the first study in 2010.
- The estimated annual cost of healthcare data breaches is as much as $5.6 billion annually
- 69% of study respondents report that the Affordable Care Act increases risk to patient privacy and security

---

1 [https://www.cms.gov/EHRIncentivePrograms](https://www.cms.gov/EHRIncentivePrograms)
2 OCR HIPAA Audit Program Protocol, Section §164.308.
Establish a Risk-based Approach with Attack Intelligence

Traditional security solutions are unable to produce actionable information, related to sensitive assets such as patient data stores or medical record application servers. This leaves healthcare organizations with unmanageable amounts of potential threats and unachievable remediation plans. Healthcare organizations require actionable risk information.

Core Security is able to isolate your sensitive assets and model the most likely path an attacker might take to reach them. Using a patented attack path planner, Core Security correlates known exploits, attack patterns, network and security data, with identified vulnerabilities. In addition to simulation, the patented attack engine can be used for automated live testing or targeted manual testing. This approach results in demonstrable attack paths to critical healthcare assets, such as an EHR database and an achievable remediation plan for IT operations.

Leading Healthcare Institution Benefits from Attack Intelligence

One prominent academic healthcare institution in the U.S. needed to prepare for a HIPAA audit, better identify vulnerabilities to their critical assets, and ultimately prove their ability to conduct an effective risk assessment. They leveraged the Core Security Attack Intelligence platform to consolidate multiple security point products, resulting in significantly reduced IT costs and a streamlined approach to managing risk.

With Core Security, this leading healthcare institution was able to prioritize their massive list of network and system vulnerabilities. Instead of attempting to remediate all vulnerabilities from periodic scans, they opted to use Core Security to focus on the threats along potential attack paths to their ePHI and EHR assets. With attack intelligence, they were able to implement an effective risk management program and demonstrate adequate risk assessments.