Solution Brief

HIPAA Readiness Workshop

Educating clients on Security Rule (SR) 45 for HIPAA compliance.

How do you maintain HIPAA compliance and avoid common HIPAA violations?

Healthcare organizations have instituted numerous cybersecurity and privacy tools, controls, and protocols to comply with Health Insurance Portability and Accountability Act (HIPAA). Yet according to the HIPAA Journal, the most common violations include failure to perform an organization-wide risk analysis, lack of a risk management process, insufficient electronic Protected Health Information (ePHI) access controls, failure to use encryption or an equivalent measure to safeguard ePHI on portable devices, and going past 60-day deadlines for issuing breach notifications.

Maintaining continuous vigilance is key to reducing your organization's risk of HIPAA violations, fines, and damaged reputation. Is your security staff ready to carry out this task?

BlueVoyant's HIPAA Readiness Workshop includes four phases:

- A brief overview of where we have been and where we are headed in cybersecurity and the healthcare industry.
- Illustrations of how various factors influence risk.
- A review of our expert approach to identifying key cyber strengths and vulnerabilities.
- An exercise to clarify your strengths and vulnerabilities, resulting in a findings and recommendations report.

BlueVoyant Differentiators

- BlueVoyant is an American Hospital Association (AHA) Preferred Cybersecurity Service Provider (APCP) for Cyber Risk Management and Managed Detection and Response (MDR) services for hospital and healthcare members.
- Our maturity model approach combines BlueVoyant's tailored risk-based assessment (people, process, technology, and governance) with HIPAA Security Rule 45 to eliminate the confusion associated with the requirements necessary to reach your compliance goals.
- Our highly experienced team helps you understand the strengths and vulnerabilities in your overall security plan and then develops recommendations based on our proprietary methods layered onto the HIPAA guidance.
- Our BlueVoyant Liquid: PS™ consultants have extensive frontline experience in helping organizations reach the required or desired level of maturity for their cyber programs.

BlueVoyant

BlueVoyant's HIPAA Readiness Workshop Phases:

Information gathering
Prior to the workshop, BlueVoyant will send your organization a survey to collect some essential, non-proprietary data to conduct basic cybersecurity risk analysis and tailor the workshop to the client's particular circumstances.

Compliance-based cybersecurity discussion
The team will discuss lessons learned in building a robust cybersecurity program, best practices for right-sized cybersecurity investment utilizing your compliance requirements, and how a maturity-based approach eliminates confusion — on where to start, how to measure success, while ensuring orchestration among different security elements within the program.

Build Common Understanding
Illustrate how various factors influence risk, discuss the factors present in the client's environment, and build high-level consensus on organizational maturity level.

Baseline current state vs. ideal state
Using results from the survey and discussion, BlueVoyant will lead an exercise designed to clarify the client's strengths and vulnerabilities, factoring in existing investments and practices. A high-level understanding of the client's security maturity and possible compliance gaps are the goals of this exercise.

Recommendations
For organizations required to be in compliance with HIPAA SR 45, we'll use the HIPAA Cyber Assessment to determine how BlueVoyant can help you maintain compliance objectives and guide your organization on what BlueVoyant proprietary software and services are needed to be added to your existing technical stack to help you obtain and maintain compliance. This will help right-size your cybersecurity program to meet the key HIPAA compliance requirements.

Should you need help with remediating any gaps in your program, BlueVoyant's integrated team of professionals are prepared to help you reach and maintain your ideal security maturity.

Ready to get started? Get in touch.

BlueVoyant combines internal and external cyber defense capabilities into an outcomes-based platform called BlueVoyant Elements™. Elements is cloud-native and continuously monitors your network, endpoints, attack surface, and supply chain plusthe clear, deep, and dark web for vulnerabilities, risks, and threats; and takes action to protect your business, leveraging both machine learning-driven automation and human-led expertise. Elements can be deployed as independent solutions or together as a full-spectrum cyber defense platform. BlueVoyant's approach to cyber defense revolves around three key pillars — technology, telemetry, and talent — that deliver industry-leading cybersecurity to more than 700 customers across the globe.

To learn more about BlueVoyant, please visit our website at **www.bluevoyant.com** or email us at **contact@bluevoyant.com**

BlueVoyant