Healthcare Cybersecurity & Patient Data Protection Training Course

Ref: #CYB6584

Course Introduction / Overview:

This comprehensive training course is designed to provide healthcare and IT professionals with the essential knowledge and practical skills needed to secure patient data and ensure regulatory compliance. Healthcare organizations are prime targets for cyberattacks due to the highly sensitive and valuable nature of Protected Health Information (PHI). This program goes beyond a general overview of cybersecurity to focus on the unique challenges, threats, and legal requirements of the healthcare industry. Participants will learn how to implement robust security measures, manage risks to electronic health records (EHR), and ensure compliance with key regulations like HIPAA and HITECH. We will cover topics like network security, access control, and incident response, all within the specific context of a healthcare environment. Drawing from the academic research of renowned authors like Ross Anderson and his foundational book "Security Engineering," which emphasizes a systems-level approach to security, this program provides a strategic and practical framework for safeguarding patient data. This course at BIG BEN Training Center will empower you to build a secure and trustworthy healthcare system.

Target Audience / This training course is suitable for:

- Healthcare IT professionals.
- Health Information Managers.
- Compliance and privacy officers.
- Cybersecurity analysts.
- Hospital and clinic administrators.
- Medical records staff.
- Risk managers.

Target Sectors and Industries:

- Hospitals and clinics.
- Pharmaceutical companies.
- Health insurance providers.
- Medical device manufacturers.
- Telehealth providers.
- Government agencies and equivalents.
- Public health organizations.

Target Organizations Departments:

- Health Information Systems.
- Information Security.
- Compliance and Risk Management.
- Medical Records.
- IT.
- Legal.
- Patient Services.

Course Offerings:

By the end of this course, the participants will have able to:

- Ensure compliance with HIPAA and HITECH.
- Implement a robust patient data protection strategy.
- Secure electronic health records (EHR) and medical devices.
- Develop and test an incident response plan.
- Manage access controls for sensitive information.
- Conduct a risk assessment of a healthcare system.
- Educate staff on cybersecurity best practices.

Course Methodology:

This training course at BIG BEN Training Center uses a scenario-based and highly practical methodology. The program combines expert-led sessions with hands-on labs that simulate real-world healthcare network environments. Participants will work through complex scenarios, such as a ransomware attack on a hospital or a data breach involving patient records. The course emphasizes a proactive and patient-centric approach. It teaches participants how to not only respond to threats but also how to build a culture of security awareness among all staff. The instructor will provide expert guidance and feedback on each scenario, ensuring that you develop the critical thinking and problem-solving skills required for protecting sensitive patient data. This approach ensures the knowledge and skills gained are directly applicable to the unique challenges of the healthcare sector.

Course Agenda (Course Units):

Unit One: The Healthcare Threat Landscape

- Unique cybersecurity risks for healthcare.
- The value of Protected Health Information (PHI).
- Common attack vectors (e.g., ransomware, phishing).
- The importance of data integrity and availability.
- The convergence of IT and medical devices.
- Cybercrime and patient safety.
- Case study: a hospital network outage.

Unit Two: HIPAA and Healthcare Compliance

- Introduction to HIPAA.
- HIPAA Security Rule vs. Privacy Rule.
- The HITECH Act.
- Breach notification and reporting requirements.
- Managing business associate agreements.
- Conducting a HIPAA risk analysis.
- Practical lab: a HIPAA compliance audit.

Unit Three: Securing Health Information Systems

- Securing Electronic Health Records (EHR) systems.
- Access controls and user authentication.
- Data encryption and at-rest protection.
- Network segmentation for medical devices.
- Vulnerability management.
- Securing telehealth and remote patient monitoring.
- Practical lab: a system hardening exercise.

Unit Four: Incident Response and Threat Mitigation

- Creating an incident response plan for healthcare.
- Steps to take during a data breach.
- Communicating with patients and regulatory bodies.
- Digital forensics in a healthcare context.
- Threat hunting and monitoring.
- Security awareness training for all staff.
- Case study: a simulated data breach.

Unit Five: The Future of Healthcare Security

- The role of AI and machine learning in security.
- Securing the Internet of Medical Things (IoMT).
- Predictive analytics for threat detection.
- The future of patient data privacy.
- Emerging threats in healthcare.
- Final project: a comprehensive security plan.
- Continuous compliance.
- Frequently Asked Questions:

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

With the rise of interconnected medical devices and the Internet of Medical Things, how can healthcare organizations manage the security of devices that are often difficult to patch and that may not have traditional security controls?

What unique qualities does this course offer compared to other courses?

This course stands out by providing a unique and vital focus on cybersecurity specifically for the healthcare sector. Unlike generic security programs, this training addresses the distinct vulnerabilities, legal requirements, and ethical considerations faced by hospitals, clinics, and other healthcare organizations. The curriculum is built around a practical, patient-centric approach. It teaches you how to not only respond to threats but also how to build a security and compliance program that protects patient privacy. The emphasis on legal frameworks like HIPAA and on creating a culture of security awareness distinguishes this course from others. It is for professionals who are ready to move beyond traditional IT security to protect one of our most sensitive types of data.