Comprehensive Healthcare Cybersecurity and Patient Data Protection Training Course

Ref: #HSM4708

Course Introduction / Overview:

The increasing digitalization of healthcare has created a new frontier of risk, making cybersecurity and patient data protection more critical than ever before. This training course is designed to equip healthcare professionals with the knowledge and skills needed to safeguard sensitive patient information and protect their organizations from cyber threats. Participants will explore everything from understanding common cyberattacks to implementing a robust data protection framework. The curriculum addresses the importance of adhering to strict regulatory requirements like HIPAA and GDPR. As noted by academic author Dr. Anna L. Wieman in her book "Healthcare Informatics: Managing Data and Information Systems," a secure information system is foundational to providing quality patient care and maintaining trust. BIG BEN Training Center is proud to offer this program, which moves beyond general IT security to focus on the unique vulnerabilities and compliance challenges of the healthcare industry. You will learn to conduct risk assessments, develop incident response plans, and create a culture of security awareness among your staff. This course empowers you to be a key defender of your organization’s digital assets and, most importantly, your patients' privacy.

Target Audience / This Training Course is Suitable for:

- Healthcare IT and cybersecurity professionals.
- Hospital administrators and managers.
- Privacy officers and compliance managers.
- Data and records management staff.
- Clinical staff and physicians.
- Medical practice owners.
- Government health officials.

Target Sectors and Industries:

- Hospitals and medical centers.
- Public health organizations and government agencies.
- Medical clinics and private practices.
- Health insurance companies.
- Medical technology and software firms.
- Pharmaceutical companies.
- Long-term care facilities.

Target Organizations Departments:

- Information technology and security departments.
- Legal and compliance departments.
- Health information management.
- Risk management departments.
- Administration and management.
- Clinical and patient care departments.
- Finance and billing departments.

Course Offerings:

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

- Assess and mitigate cybersecurity risks in a healthcare setting.
- Implement a framework for protecting electronic patient data.
- Ensure compliance with major data privacy regulations.
- Develop and execute a cyber incident response plan.
- Educate and train staff on security best practices.
- Protect medical devices and Internet of Things (IoT) from vulnerabilities.
- Create a strong security culture within their organization.

Course Methodology:

This training course uses a blend of case studies and practical workshops. Participants will analyze real-world cyberattack scenarios and work in groups to develop a response strategy. The curriculum includes hands-on workshops on conducting risk assessments, identifying common vulnerabilities, and creating a data breach communication plan. Our instructors are seasoned cybersecurity experts with extensive experience in the healthcare sector who will share their knowledge and provide direct feedback. BIG BEN Training Center is committed to creating a collaborative and interactive environment where you can learn from your peers and practice new skills. The course is designed to be highly practical, ensuring you leave with the tools and confidence to protect your organization and your patients' data from evolving threats.

Course Agenda (Course Units):

Unit One: The Healthcare Cybersecurity Landscape.

- The unique threats to healthcare organizations.
- Understanding common cyberattacks.
- The value of protected health information (PHI).
- Key regulations: HIPAA, GDPR, and HITECH Act.
- Building a business case for cybersecurity investment.
- The importance of a risk-based approach.
- Case study: a major healthcare data breach.

Unit Two: Protecting Patient Data.

- Developing and implementing a data protection framework.
- Access control and user authentication.
- Data encryption and secure data transmission.
- Managing electronic health records (EHR) securely.
- The role of secure data storage.
- Safeguarding patient privacy in the digital world.
- Workshop: data mapping and flow exercise.

Unit Three: Technical and Operational Security.

- Securing networks and endpoints.
- Vulnerability management and penetration testing.
- The risks of medical device security and IoT.
- Cloud security for healthcare.
- Developing an incident response and recovery plan.
- Security best practices for remote work.
- Tabletop exercise: a simulated ransomware attack.

Unit Four: Compliance, Governance, and Training.

- Building a culture of security.
- Creating and enforcing security policies and procedures.
- Training staff on security awareness and phishing prevention.
- The role of the chief information security officer (CISO).
- Conducting a security audit.
- Responding to regulatory audits and investigations.
- Group discussion: the challenges of securing legacy systems.

Unit Five: The Future of Healthcare Cybersecurity.

- Threat intelligence and future trends.
- The role of AI and machine learning in security.
- Blockchain and its application in healthcare.
- Developing a long-term cybersecurity roadmap.
- The future of telemedicine and security.
- Ethical hacking for a stronger defense.
- Final project: a comprehensive cybersecurity roadmap for a healthcare facility.

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:

How can healthcare organizations build a proactive and resilient cybersecurity program when faced with the dual challenges of limited budgets and a constantly evolving threat landscape?

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

This training course stands out by providing a deep and practical division into healthcare cybersecurity and patient data protection. Unlike generic IT security courses, it addresses the specific regulatory requirements and unique vulnerabilities of the medical field. Our program emphasizes compliance with HIPAA and GDPR, the security of electronic health records (EHR), and the protection of connected medical devices. We use hands-on workshops and real-world incident simulations to give you the skills needed to proactively defend your organization. This course is for professionals who want to understand how to build a strong security culture that protects not only their organization's reputation and finances but also the privacy and trust of their patients.