Healthcare Cybersecurity and Patient Data Privacy Training Course



23 - 27 Nov 2026

Boston

7500 € (Per Person)

Ref: #HSM9113_105071

Course Introduction / Overview:

In an era where digital transformation is reshaping healthcare, the sanctity of patient data and the resilience of healthcare systems are paramount. This training course provides a comprehensive exploration of the critical intersection between cybersecurity and information privacy within the unique context of the healthcare industry. As threats like ransomware and sophisticated phishing attacks increasingly target healthcare organizations, a proactive and educated approach to security is no longer optional but essential for patient safety and institutional integrity. This program, offered by BIG BEN Training Center, is meticulously designed to address these challenges head-on. We will delve into the complex regulatory landscape, including HIPAA, HITECH, and GDPR, ensuring participants understand their compliance obligations. Drawing on principles discussed by experts like Dr. Kevin Fu in the field of medical device security, the course moves beyond theory. It provides practical strategies for securing electronic health records (EHR), protecting the Internet of Medical Things (IoMT), and developing robust incident response plans. Participants will gain the knowledge to build a resilient security posture, safeguarding sensitive patient information and ensuring the continuity of care in an increasingly connected world.

Target Audience / This training course is suitable for:

- Healthcare IT Professionals.
- Information Security Officers and Analysts.
- Hospital and Clinic Administrators.
- Compliance and Privacy Officers.
- Clinical Staff (Doctors, Nurses, Technicians).
- Medical Records Managers.
- Healthcare Risk Managers.
- Health Information Management (HIM) Professionals.
- Medical Device Engineers.
- Pharmaceutical IT Staff.
- Health Insurance Professionals.

Target Sectors and Industries:

- Hospitals and Healthcare Systems.
- Private Medical Practices and Clinics.
- Pharmaceutical and Biotechnology Companies.
- Medical Device Manufacturing Companies.
- Health Insurance Providers.
- Telehealth and Digital Health Service Providers.
- Medical Research Institutions.
- Governmental Health Agencies and Public Health Organizations.
- Third-party Healthcare Service Providers and Business Associates.
- Long-term Care and Rehabilitation Facilities.

Target Organizations Departments:

- Information Technology (IT) and Information Security.
- Compliance and Regulatory Affairs.
- Legal Department.
- Clinical Operations and Patient Care Services.
- Risk Management.
- Administration and Executive Management.
- Human Resources (for employee training and policy enforcement).
- Health Information Management (HIM).
- Procurement (for vetting third-party vendors).
- Research and Development.

Course Offerings:

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

- Analyze the unique cybersecurity threat landscape facing the healthcare sector.
- Interpret and apply key regulations such as HIPAA, HITECH, and GDPR to healthcare operations.
- Develop and implement robust security policies for protecting Electronic Health Records (EHR).
- Assess and mitigate security risks associated with the Internet of Medical Things (IoMT).
- Implement effective access control and data encryption strategies for patient information.
- Design a comprehensive incident response plan for data breaches and cyber-attacks.
- Conduct thorough risk assessments and vulnerability management for clinical systems.
- Secure telehealth platforms and remote patient monitoring technologies.
- Evaluate and manage cybersecurity risks posed by third-party vendors and partners.
- Foster a culture of security and privacy awareness throughout a healthcare organization.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be immersive, practical, and highly interactive, moving beyond traditional lecture-based learning. This course employs a blended approach that combines expert-led instruction with hands-on, real-world scenarios. Participants will engage in detailed case study analyses of major healthcare data breaches, deconstructing the attack vectors and response strategies to learn critical lessons. Collaborative group workshops will challenge teams to develop security policies, conduct mock risk assessments, and draft incident response plans based on realistic healthcare settings. Interactive sessions, Q&A panels, and peer-to-peer discussions are integrated throughout the five days to foster a dynamic learning environment where participants can share experiences and solve problems collectively. We emphasize practical application, ensuring that the skills and knowledge acquired are directly transferable to the participant's professional role. This active learning model guarantees a deeper understanding of complex concepts and equips attendees with the confidence to implement effective cybersecurity and privacy controls within their own organizations.

Course Agenda (Course Units):

Unit One: The Healthcare Cybersecurity and Regulatory Landscape

- Introduction to Healthcare Information Security.
- Understanding the Unique Threats to the Healthcare Sector.
- The CIA Triad (Confidentiality, Integrity, Availability) in a Clinical Context.
- Deep Dive into HIPAA Security and Privacy Rules.
- Exploring the HITECH Act and Breach Notification Rules.
- GDPR's Impact on Global Healthcare Operations.
- Ethical Considerations in Patient Data Privacy.

Unit Two: Securing Healthcare Systems and Infrastructure

- Network Security Fundamentals for Clinical Environments.
- Securing Electronic Health Record (EHR) Systems.
- Protecting the Internet of Medical Things (IoMT) and Biomedical Devices.
- Cloud Computing Security for Healthcare Data.
- Implementing Secure Remote Access and Telehealth Platforms.
- Physical Security Controls for Data Centers and Medical Facilities.
- Vulnerability Management and Patching Protocols.

Unit Three: Protecting and Governing Sensitive Patient Data

- Data Classification and Handling of Protected Health Information (PHI).
- Advanced Encryption Techniques for Data at Rest and in Transit.
- Identity and Access Management (IAM) in Healthcare.
- Implementing the Principle of Least Privilege.
- Strategies for Data Loss Prevention (DLP).
- Secure Data Disposal and Media Sanitization.
- Auditing and Monitoring Access to Patient Records.

Unit Four: Risk Management and Incident Response

- Conducting a Healthcare-Specific Security Risk Analysis.
- Developing and Implementing a Risk Management Program.
- Building a Comprehensive Incident Response Plan.
- Managing and Reporting a Data Breach.
- Digital Forensics in a Healthcare Investigation.
- Business Continuity and Disaster Recovery Planning for Hospitals.
- Developing Effective Security Awareness and Training Programs.

Unit Five: Advanced Topics and Future-Proofing Healthcare Security

- Managing Third-Party and Supply Chain Cyber Risk.
- The Role of Artificial Intelligence (AI) in Healthcare Cybersecurity.
- Threat Intelligence and Proactive Threat Hunting.
- Developing Secure Healthcare Applications and Software.
- Preparing for Cybersecurity Audits and Certifications.
- Building a Resilient, Security-First Culture.
- The Future of Healthcare Cybersecurity and Emerging Threats.

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:

As telehealth and AI become more integrated into patient care, how can healthcare organizations balance the drive for innovation with the fundamental ethical obligation to protect patient privacy?

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

This course distinguishes itself by offering a holistic and pragmatic perspective specifically tailored to the complex healthcare environment. While many programs focus narrowly on either technical controls or regulatory compliance, our curriculum seamlessly integrates both, recognizing that effective security is a fusion of technology, policy, and people. We move beyond theoretical discussions of HIPAA to explore its practical application in challenging scenarios like securing legacy medical devices or managing cloud-based EHR systems. A key differentiator is our dedicated focus on emerging threat vectors, including the Internet of Medical Things (IoMT) and telehealth platforms, which are often overlooked in standard cybersecurity training. The methodology is rooted in real-world case studies of actual healthcare breaches, allowing participants to learn from tangible successes and failures. Rather than just listing security tools, we empower participants with the strategic thinking needed to conduct comprehensive risk assessments and build a resilient, proactive security culture. This approach ensures that attendees leave not just with knowledge, but with the actionable wisdom required to protect patient data and ensure continuity of care in a high-stakes industry.