



SECURE ELECTRONIC MEDICAL RECORDS MANAGEMENT AND COMPLIANCE TRAINING COURSE

21 - 25 DEC 2026

KUALA LUMPUR

5200 € (PER PERSON)

REF: #HOS4775_1 13348



COURSE INTRODUCTION / OVERVIEW:

The transition to Electronic Medical Records (EMR) has revolutionized healthcare delivery, offering unprecedented efficiency and improved patient outcomes. However, this digital shift introduces significant challenges related to data security and regulatory compliance. This comprehensive course is designed to equip healthcare professionals with the essential knowledge and skills to manage EMR systems securely and effectively, ensuring the confidentiality, integrity, and availability of sensitive patient information. Drawing upon foundational principles discussed by leading experts like William R. Hersh in works such as "Health Informatics: Practical Guide," this program delves into the technical, administrative, and physical safeguards required to protect electronic protected health information (ePHI). Participants will explore the complexities of regulatory frameworks like HIPAA and learn to implement robust security protocols. BIG BEN Training Center has developed this curriculum to move beyond theoretical knowledge, focusing on practical application through real-world scenarios, risk assessment techniques, and incident response planning, empowering attendees to build a resilient and compliant healthcare data environment.

TARGET AUDIENCE / THIS TRAINING COURSE IS SUITABLE FOR:

- Healthcare Administrators and Managers.
- Medical Records and Health Information Technicians.
- IT Professionals and Security Specialists in Healthcare.
- Clinical Staff including Doctors, Nurses, and Physician Assistants.
- Healthcare Compliance and Privacy Officers.
- Medical Billing and Coding Specialists.
- Practice Managers in Clinics and Hospitals.
- Healthcare Legal and Risk Management Personnel.

TARGET SECTORS AND INDUSTRIES:

- Hospitals and Integrated Health Systems.
- Private Medical Practices and Specialty Clinics.
- Long-Term Care Facilities and Nursing Homes.
- Health Insurance and Payer Organizations.
- Medical Billing and Third-Party Administrator Companies.
- Governmental Health Agencies and Public Health Organizations.
- Pharmaceutical and Biomedical Research Companies.

- Healthcare Technology and EMR Software Vendors.

TARGET ORGANIZATIONS DEPARTMENTS:



- Information Technology (IT) and Cybersecurity.
- Health Information Management (HIM) and Medical Records.
- Compliance, Legal, and Privacy Departments.
- Clinical Operations and Patient Services.
- Administration and Executive Management.
- Quality Assurance and Improvement.
- Risk Management and Internal Audit.
- Finance and Billing Departments.

COURSE OFFERINGS:

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

- Develop and implement comprehensive security policies for EMR systems.
- Ensure organizational compliance with key healthcare regulations like the HIPAA Security and Privacy Rules.
- Conduct thorough risk analyses to identify and mitigate vulnerabilities in healthcare IT infrastructure.
- Master the principles of access control to protect electronic protected health information (ePHI).
- Design and execute effective incident response and data breach notification plans.
- Utilize encryption and other technical safeguards to secure data both at rest and in transit.
- Establish robust audit control mechanisms to monitor and record activity in information systems.
- Promote a culture of security awareness and data stewardship within their organization.
- Evaluate the security implications of emerging technologies like telehealth and mobile health applications.
- Manage EMR data integrity, retention, and secure disposal according to best practices.

COURSE METHODOLOGY:

The training methodology at BIG BEN Training Center is designed to be immersive, interactive, and highly practical, ensuring that participants can directly apply their learning to their professional roles. This course moves beyond traditional lectures by integrating a dynamic blend of expert-led presentations, in-depth case study analyses of real-world healthcare data breaches, and collaborative group discussions. Participants will engage in hands-on workshops focused on conducting risk assessments, developing security policies, and simulating incident response scenarios. Interactive Q&A sessions encourage active participation and allow for the clarification of complex regulatory and technical concepts. Team-based exercises will challenge attendees to solve practical EMR security problems, fostering critical thinking and collaborative skills. The instructor will provide continuous feedback and facilitate knowledge sharing among peers from diverse healthcare backgrounds. This multifaceted approach ensures a comprehensive understanding of EMR management and data security, equipping participants with both the strategic insights and the practical tools needed to protect sensitive patient data effectively.

COURSE AGENDA (COURSE UNITS):

UNIT ONE: FOUNDATIONS OF EMR AND HEALTHCARE INFORMATICS

- Introduction to Electronic Medical Records (EMR) and Electronic Health Records (EHR).
- The Evolution of Health Information Technology.
- Key Components and Functions of an EMR System.
- Benefits and Challenges of EMR Implementation.
- The Regulatory Landscape for Health Information.
- Understanding Protected Health Information (PHI).
- Ethical Considerations in Digital Health Record Management.
- The Role of Data Standards and Interoperability.



UNIT TWO: PRINCIPLES OF HEALTHCARE DATA SECURITY

- The CIA Triad: Confidentiality, Integrity, and Availability.
- Administrative, Physical, and Technical Safeguards.
- Access Control Models and Best Practices.
- User Authentication and Authorization Mechanisms.
- Fundamentals of Data Encryption for PHI.
- Securing Networks and Transmission Security.
- Protecting Mobile Devices and Endpoints in a Healthcare Setting.
- Understanding Malware and Social Engineering Threats in Healthcare.

UNIT THREE: HIPAA COMPLIANCE AND REGULATORY FRAMEWORKS

- Deep Dive into the HIPAA Privacy Rule.
- Understanding the HIPAA Security Rule Requirements.
- Navigating the HIPAA Breach Notification Rule.
- The Role of the HITECH Act in Strengthening Privacy and Security.
- Business Associate Agreements and Third-Party Vendor Management.
- Patient Rights and Authorizations under HIPAA.
- Conducting a HIPAA Security Risk Analysis.
- Global Perspectives: GDPR and its Impact on Healthcare Data.

UNIT FOUR: RISK MANAGEMENT AND INCIDENT RESPONSE

- Developing a Healthcare Information Security Risk Management Program.
- Methods for Identifying and Assessing Security Vulnerabilities.
- Implementing Risk Mitigation Strategies and Controls.
- Creating and Testing an Incident Response Plan (IRP).
- Steps for Containing, Eradicating, and Recovering from a Security Breach.
- Forensic Investigation Basics in a Healthcare Context.
- Developing a Disaster Recovery and Business Continuity Plan.
- Training and Awareness Programs for Staff.

UNIT FIVE: ADVANCED E-MEDICAL RECORDS MANAGEMENT AND GOVERNANCE

- Implementing Audit Controls and Reviewing System Activity Logs.
- Data Governance Frameworks for Healthcare Organizations.
- Ensuring Data Integrity and Accuracy in EMR Systems.
- Policies for EMR Data Retention and Secure Destruction.
- Security Considerations for Telehealth and Remote Patient Monitoring.
- The Impact of Cloud Computing on EMR Security.
- Future Trends: AI, Machine Learning, and Blockchain in Healthcare Data Security.
- Building and Maintaining a Culture of Security and Compliance.



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 healthcare becomes increasingly interconnected through Health Information Exchanges (HIEs), how can organizations balance the critical need for data interoperability with the non-negotiable requirement for patient data privacy and security?

WHAT UNIQUE QUALITIES DOES THIS COURSE OFFER COMPARED TO OTHER COURSES?

This course distinguishes itself by adopting a holistic, strategy-focused approach that integrates technical security with organizational policy and clinical workflow. Unlike programs that concentrate solely on IT controls or software features, this training emphasizes the development of a comprehensive security culture. We delve into the "why" behind the regulations, empowering participants not just to follow a checklist but to conduct nuanced risk assessments tailored to their specific operational environment. The curriculum is built around real-world case studies of healthcare data breaches, allowing for a practical examination of what went wrong and how such incidents could have been prevented. A significant focus is placed on proactive risk management and incident response planning, equipping leaders with the skills to prepare for and manage crises effectively. Furthermore, the course content bridges the gap between the IT department, clinical staff, and administration, fostering a common language and understanding of security responsibilities across the entire organization. This strategic, interdisciplinary perspective ensures that participants leave with actionable insights to build a truly resilient and compliant data protection program.