SEC474: **Building A Healthcare Security & Compliance Program**

2 Day Course	12 CPEs	Laptop Required

You Will Be Able To

- Tackle the challenges at hand – many HIPAA compliance regulations run counter to business objectives, so we will explore why this is and how to overcome the issue
- Interpret the Security Rule text in-depth, including an analysis of every line item of the regulation and what it means to your organization
- Draft sound policy that supports business as well as compliance objectives
- Perform a risk assessment, enumerate threat data, analyze vulnerabilities, and select proper safeguards to lower risk
- Define the value of the compliance program for the organization
- Create a culture of compliance
- Establish lines of communication and reporting channels
- Understand the value of internal monitoring and auditing by learning the key components of a continuous monitor reporting and improvement program
- Promote a culture of compliance

Who Should Attend

- Healthcare CSO/CIO/CISOs
- Information security managers/ administrators
- IT security analysts/managers/directors
- HIPAA compliance officers
- Compliance analysts
- Medical records supervisors
- Compliance auditors
- Healthcare security consultants
- IT managers in healthcare organizations

What You Will Receive

- Physical and digital workbooks
- Virtual machine tailored to the course
- HIPAA-based risk assessment tool

One of the challenges organizations face in complying with the Health Insurance Portability and Accountability Act (HIPAA) is that the act's regulatory and privacy standards are not prescriptive enough to help organizations successfully build an effective security and compliance program. Audit and assessment engagements with government agencies such as the Office of Civil Rights (OCR) and with state attorney generals during and after reportable data breaches or privacy-related security incidents can be overwhelming for organizations to navigate without previous knowledge or experience.

To address tight budget restrictions, many healthcare organizations promote security and compliance team members from within the organization in order to cultivate and retain talent internally. These professionals have a wide range of experience and skill sets. The SANS SEC474 course can help organizations level-set and prepare healthcare compliance and security by sharing first-hand knowledge and experiences.

The goal of this course is to show that HIPAA compliance in itself is neither an antidote nor a cure for the shortcoming of an organization's healthcare security. The ultimate goal is to develop, maintain, and demonstrate a secure environment for the organization by implementing repeatable processes based on industry best practices. When that is achieved, evidence of HIPAA compliance is a result of those efforts.

Healthcare organizations in the United States face two major challenges: first, to properly secure the organization from tactical risk, and second, to achieve compliance with the array of government regulations known as HIPAA. This course will help students develop the skills to make measurable improvements to the overall security posture of their organization's IT infrastructure while also building and maintaining a compliance program. Using the safeguards of the HIPAA Security Rule along with the NIST Framework 800-66 to identify and assess risk, students will learn how to report progress on their compliance activities and their security value in support of the organization's mission.

Students will gain skills and knowledge in SEC474 that they will be able to use on their first day back at work. Students will leave the classroom knowing what it takes to establish and nurture a culture of compliance where both compliance and business objectives are promoted as a singular goal. They will be able not only to assess compliance, but also to measure the maturity and effectiveness of compliance activities.

This course will prepare you to:

- Take steps to meet compliance standards, particularly those of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and Health Information Technology for Economic and Clinical Health Act (HITECH)
- Protect your healthcare organization from cyber-threats, unintended data disclosures, and mishandling of data in the enterprise
- Understand the most prevalent security concerns specifically around the healthcare industry such as data disclosures, ransomware, unauthorized access and modification, incident response, and business continuity planning
- Apply the HIPAA Security Rule in practice
- Build an organizational security plan
- Understand the job roles in a compliance program

Section Descriptions

SECTION 1: Risk and Compliance

This course section introduces the student to the HIPAA regulations and how they support, and occasionally conflict with, organizational goals of patient care and privacy. The student will learn the fundamentals of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), HITECH, and the Omnibus Rule. This course focuses on effectiveness and maturity by exploring the following key questions:

- Is there written documentation?
- Is there a process in place?
- Is the process automated or manual?
- Can effectiveness be demonstrated with metrics?

We will also explore strategies to align with healthcare objectives and focus on the effectiveness and maturity of security activities. Students will learn the importance of physical security in safeguarding electronic protected health information (ePHI). The section concludes with a discussion on defining the value of the compliance program to align with business needs.

EXERCISES:

- **Rules of the Road:** Using raw field data from a site assessment walk-through and entering results into an assessor, this exercise ensures that students are comfortable with navigating both the assessor and ticketing provided in lab software and entering data into the most appropriate sections.
- **Identifying Vulnerabilities and Threats:** This exercise involves analyzing and prioritizing vulnerabilities in ticketing systems and referencing organizational policies and procedures. The aim is to ensure that students are comfortable with navigating the policy manager software provided in the lab virtual machine.
- **Mapping and Scoring Assessment Maturity Ratings:** Analyzing assessment report results and enter the appropriate maturity scale (1-4) based on the evidence provided. The aim is to ensure that students are familiar with the rating and scoring process within the assessor software.
- **Safeguards and Storage:** This exercise involves reviewing ticket requests and security incidents common in the healthcare industry and making appropriate decisions based on the evidence and information obtained from key departments outside of security. These skills require students to use critical thinking based on a number of key factors.
- **Measuring Response Effectiveness:** In this exercise, students will analyze a recent Ryuk Ransomware security incident report to measure response effectiveness as it relates to current trends in cybersecurity and specifically the healthcare industry. Using the Mitre ATT&CK framework, students will also have an added bonus challenge to unmask the suspected threat group responsible for the attack!

TOPICS:

- Understanding the Challenge
- HIPAA, HITECH, and the Omnibus Rule: An Exploration of the Laws and Regulations that Affect Covered Entities
- Applying the HIPAA Security Rule Using the NIST Cybersecurity Framework Security Objectives
- Exploring the Security Rule Safeguards and How to Apply Them in a Healthcare Setting
- Risk Analysis
- Types of Attacks
- Other Frameworks
- Physical Security
- Define the Value of Your Compliance Program

SECTION 2: Policy, Documentation, and Culture

This course section focuses on security and compliance efforts, including identifying key roles, contracts, and other documents. The goal is to teach the student how to design organizational structures with outcomes that ensure compliance. Students will learn the dual roles of culture and policy to ensure that compliance mandates are met. They'll also learn to use written procedures and standards to define management intent, as well as how to use training and awareness to ensure compliance. We'll wrap up the course section by examining the importance of continuous improvement and the measurement of success through continuous monitoring, auditing, and reporting. Students will learn techniques for proper communication of risk to leadership.

EXERCISES:

- **Finalizing a Telecommute Policy:** In this exercise, students will review a drafted telecommute policy that is missing key security and compliance elements. Students will need to address common challenges faced during the COVID-19 pandemic, including how to best enable remote workers to continue operations from home securely.
- **Business Impact Analysis (BIA) for Telehealth Services:** This exercise involves analyzing and reviewing a BIA for telehealth services that has been recently updated. Students will respond to an email from the IT Director on overall business impact and recovery time objective score information that is derived from the BIA.
- **Initial Assessment for Telehealth Services:** Students will review and assess three software/hardware platforms to use telehealth services and engage with patients remotely. Students will assess the security controls of each solution proposed and list pros and risks associated with the individual platforms. Then they'll make recommendations on which telehealth platform should be selected, with supporting reasoning and taking into consideration the recent guidelines issued by U.S. Department of Health and Human Services during the pandemic.
- **Reporting to Management:** In this exercise, students will review and complete missing sections of the annual BHHS Information Security Report to the executive board by looking up tickets within the ticketing system and contacting key individuals by email to obtain additional information and context to provide to the CIO for an upcoming board meeting. Students will take elements and data points gathered from previous labs to enter in final updates.

TOPICS:

- Culture and Policy
- Draft and Disseminate Written Policies
- Implement Written Procedures and Standards
- Conduct Internal Monitoring and Auditing
- Promote a Culture of Compliance
- Continuous Monitoring, Reporting, and Improvement