CERTIFIED HEALTHCARE CYBERSECURITY PROFESSIONAL (CHCSP)

Approved for Continuing Education Credit

HIMSS Certification:
This program is approved for up to 15 continuing education (CE) hours for use in fulfilling the continuing education requirements of the Certified Professional in Healthcare Information & Management Systems (CPHIMS) and the Certified Associate in Healthcare Information & Management Systems (CAHIMS).

For **CAHIMS**, you are required to obtain 45 CEs during your renewal cycle.
• A minimum of 25 of the 45 CEs must be obtained from HIMSS or HIMSS-Approved Provider activities.

For **CPHIMS**, you are required to obtain 45 CEs during your renewal cycle.
• A minimum of 25 of the 45 CEs must be obtained from HIMSS or HIMSS-Approved Provider activities.

To submit the Non-HIMSS Continuing Education Units to become CHCIO eligible or to maintain/renew your CAHIMS or CPHIMS eligible status, CLICK HERE to access further information on **HIMSS Professional Certification in Healthcare Information and Management Systems (CAHIMS, CPHIMS, and CPHIMS-CA) Renewal Requirements and Application**

Objectives:
Upon successfully completing this course, students will be able to:

- Identify how to protect valuable information assets
- List requirements of a formal cybersecurity risk management program
- Discuss Security and Compliance initiatives
- Explain how to build cybersecurity frameworks
- Define the nuance between Cybersecurity and HIPAA
- Define National CSF and HITRUST
- Explain risk-based management concepts
- Discuss the new definition of risk
- Identify cybersecurity stakeholders
- Discuss an identified risk
- Identify how to manage risk oversight
- Review the cybersecurity framework
- Describe how to perform risk analysis and program assessments

Planning & Instructional Personnel Disclosures:

All planners and instructors have completed a Biographical Data and Conflict of Interest form and have no conflicts of interest to disclose.