

Learn Cybersecurity the healthcare way

Your cybersecurity challenges are unique to healthcare.

Challenge:

Cybersecurity in a healthcare setting presents a challenge unlike other business environments. The highly sensitive nature of healthcare records makes them a particularly attractive target for cyber criminals. And a consequential breach of healthcare records can pose great risk to your enterprise.

Potential cybersecurity threats have an impact that reaches across your entire organization.

Healthcare Executive

Is there the potential for a cybersecurity threat creating a health/safety risk to my organization?

Information Technology

Can an enterprise security solution address the evolving security threats both internally and externally?

Clinical Engineering

What provisions are in place for proper medical device security in enterprise network design?

Clinical Staff

Are there cybersecurity policies in place at my facility?

Facilities Management

What are the risks and responses for lost/stolen medical equipment or any device that may contain patient data?

As the risk of data theft continues to escalate, many organizations realize that it is critical to develop a cybersecurity strategy.

Solution:

Cybersecurity Essentials for Healthcare





Cybersecurity Essentials for Healthcare

Course length: 1 hour

Delivery method: online

This course will provide a general awareness of cybersecurity and will help identify what is needed in healthcare organizations to address this current and evolving threat. Real time profile cybersecurity examples and outcome based practices for mitigation and response are presented. The “human ware” component related to security in all areas within the organization is discussed.

A holistic approach is used to provide consistent cybersecurity essential training to increase the awareness of potential risks for the entire staff. Each section of the course has a focus on a particular role as related to cybersecurity. Key learnings are reviewed for the role of Healthcare Executive, Information Technology, Clinical Engineer, Clinical Staff and Facilities Management.

Cybersecurity Essentials for Healthcare

By the end of this section, the participant should be able to:

<p>Healthcare Executive:</p> <ul style="list-style-type: none"> • Identify potential problems for cybersecurity in healthcare that are a risk to the organization • Develop a strategic plan to address the changing and evolving threats 	<p>Clinical Engineering:</p> <ul style="list-style-type: none"> • Describe what provisions are in place for proper medical device security in enterprise network design • Review policies and procedures for software updates and tracking for medical devices 	<p>Facilities Management:</p> <ul style="list-style-type: none"> • Describe risk and response for lost stolen medical devices, and/or IT devices that may contain patient data • Describe policies and procedures for all employees, families, and outside personnel
<p>Information Technology:</p> <ul style="list-style-type: none"> • Describe best practices and training for social engineering and email phishing attacks • Create policies required for Bring Your Own Device (BYOD), portable media, wireless access, and authentication audit 	<p>Clinical Staff:</p> <ul style="list-style-type: none"> • Describe the best practices for email use, PHI, BYOD, and use of portable media devices • Explain the log in and log out procedures for devices and any impact of work around solutions 	<p>For More Information, contact us: geeducation@ge.com (877) 438-4788</p>

This online program gives you power and flexibility to manage your cybersecurity education initiatives. Participants can access web-based education applications 24 hours a day, seven days a week. You also have documentation with reports of course completion and continuing education in cybersecurity.