How to Implement Cybersecurity Workforce Training

Cybersecurity Workforce Training for Medium-sized Healthcare Organizations

HHS 405(d)
Aligning Health Care Industry Security Approaches

What is cybersecurity workforce training?
Cyber workforce training is an effort to train your staff on the most common and pertinent cyber threats today. Everyone in a healthcare office or organization should receive cybersecurity training to protect patients from cyber threats.

Why is it important?
Cyber threats are constantly changing, and the threat to healthcare offices and organizations are real. The most common way for bad actors to infiltrate an organization is through the workforce with tactics such as email phishing. To keep your organization and your patients' data safe you must continuously train your staff on recent cyber tactics.

How will this keep my organization safe?
Cyber-attacks not only harm patients, but they also cause considerable reputational and financial harm to an organization. All staff of an organization, regardless of size, are the first line of defense when it comes to cyber-attacks. If you prepare your work force to recognize and identify potential cyber threats, your patients and your organization will be more secure.

Threats Training Mitigates:

- Email Phishing
- Ransomware
- Loss or Theft of Equipment
- Insider, Accidental, or Intentional Data Loss

Implementation Tips:

Ignite each manager's passion to coach their employees. Engage and train your management team. Leverage them to communicate security practices and information to staff in all areas of the organization.

Deal with the short shelf life of learning and development needs. Security information changes continuously. Implement continuous and ongoing campaigns to maintain awareness of current trends, issues, and events.

Teach employees to own their career development. Customize cybersecurity training to the needs of employees in different positions or units in the organization. Develop training that is clearly relevant to the user's job.

Provide flexible learning options. Provide options, including on-demand and mobile training solutions, that allow the workforce to schedule and complete training independently.

Build trust in organizational leadership. Leaders must be open and transparent and lead by example. Managers must demonstrate to the workforce that they are fully engaged in security strategy and committed to successful execution of security controls and techniques.

Train staff on your organization's policies for the protection of mobile devices such as laptops, tablets, or cell phones. Train your workforce on the need to report any lost or stolen endpoints to your cybersecurity department. Reporting should occur promptly so cybersecurity departments can execute the proper incident response procedures.

To learn more about how you can protect your patients from cyber threats check out the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication. Check out the available resources 405(d) has to offer by visiting our website at 405d.hhs.gov and our social media pages: **@ask405d** *on Facebook, Twitter, LinkedIn and Instagram!*