Patient Safety Awareness Week 2022: Cyber Safety is Patient Safety

HHS 405(d)
Aligning Health Care
Industry Security Approaches

Patient Safety Awareness Week is an important time of year for healthcare organization members to reflect and learn new ways to protect patients, and this also includes cyber safety. The 405(d) Program promotes that **Cyber Safety is Patient Safety**, and everyone has a role to play. Letting just one cyber threat through the physical and technological doors could be disastrous to your organization and patients.

Follow these tips to begin exercising proper cyber hygiene and protecting your patients from cyber threats. You can learn more with the *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP)* publication at 405d.hhs.gov.

Know Your Role

Every healthcare organization member has a role in cybersecurity. Reflect on what you can access: digital and physical PHI, medical devices, and more. You are an important layer of defense between patients and cyber threat actors who may try to gain access to these resources. It is also your responsibility to stay up-to-date on the newest threats, like email phishing, so you are prepared.

Update Your Devices

Don't hesitate, update! Updated devices are more secure devices. If you receive a notification from your organization's IT professionals that an update is required, run the update as soon as possible. Threat actors can infect your IT system as quickly as germs can infect your body. Make sure your devices have the most up-to-date cyber protection to keep the system healthy.

Learn Reporting Policies

Reporting phishing emails is extremely important to maintaining good cyber hygiene, but that is not the only form of reporting you should do to protect your patients. Check with your organization's cyber and IT professionals to learn their reporting policies for other issues, such as lost or stolen equipment, departing employees, and cyber incident notifications.

Secure Your Equipment

In addition to staying up to date, your equipment requires other forms of protection. Physical security of equipment is an important part of cyber safety. Your equipment houses all your patients' data. If the equipment is lost or stolen, then the data within it is lost or stolen too. Even if there are layers of security within the equipment, the cyber threat is one layer closer to your patients' valuable PHI.

Protect Patient Data

Patient data is valuable to both your organization and threat actors that want to exploit that data. Learn your organization's procedures for storing, encrypting, and transmitting patient data, then follow those procedures as though your patients' safety depend on it.

Cyber Safety is Patient Safety

As you can see, cybersecurity requires multiple layers of protection. **YOU** are one of the most important layers to protect patients from cyber threats because you can implement and oversee other layers. Follow along with the 405(d) Program on social media **@ask405d** for the latest cybersecurity awareness products and resources tailored to the healthcare and public health sector. Don't forget: **Cyber Safety is Patient Safety.**