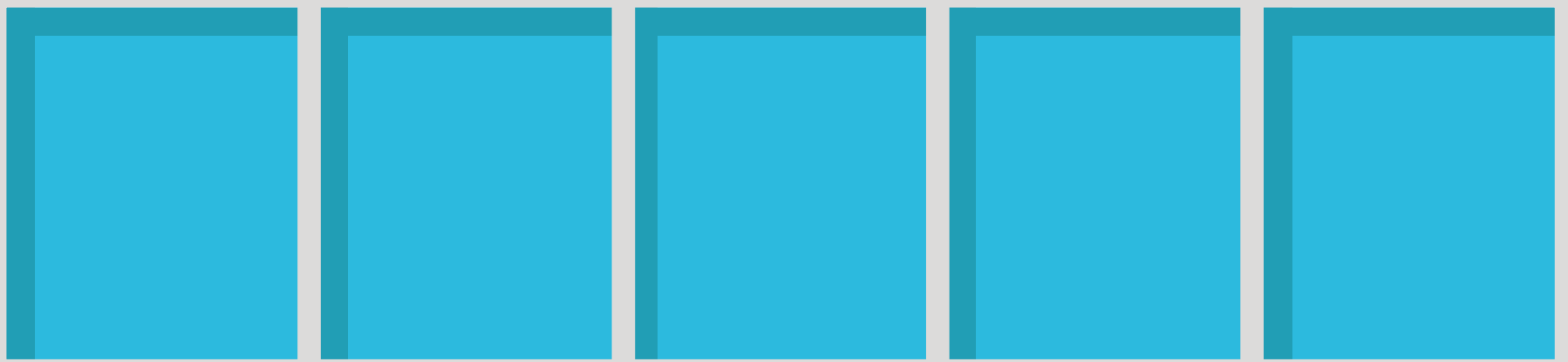
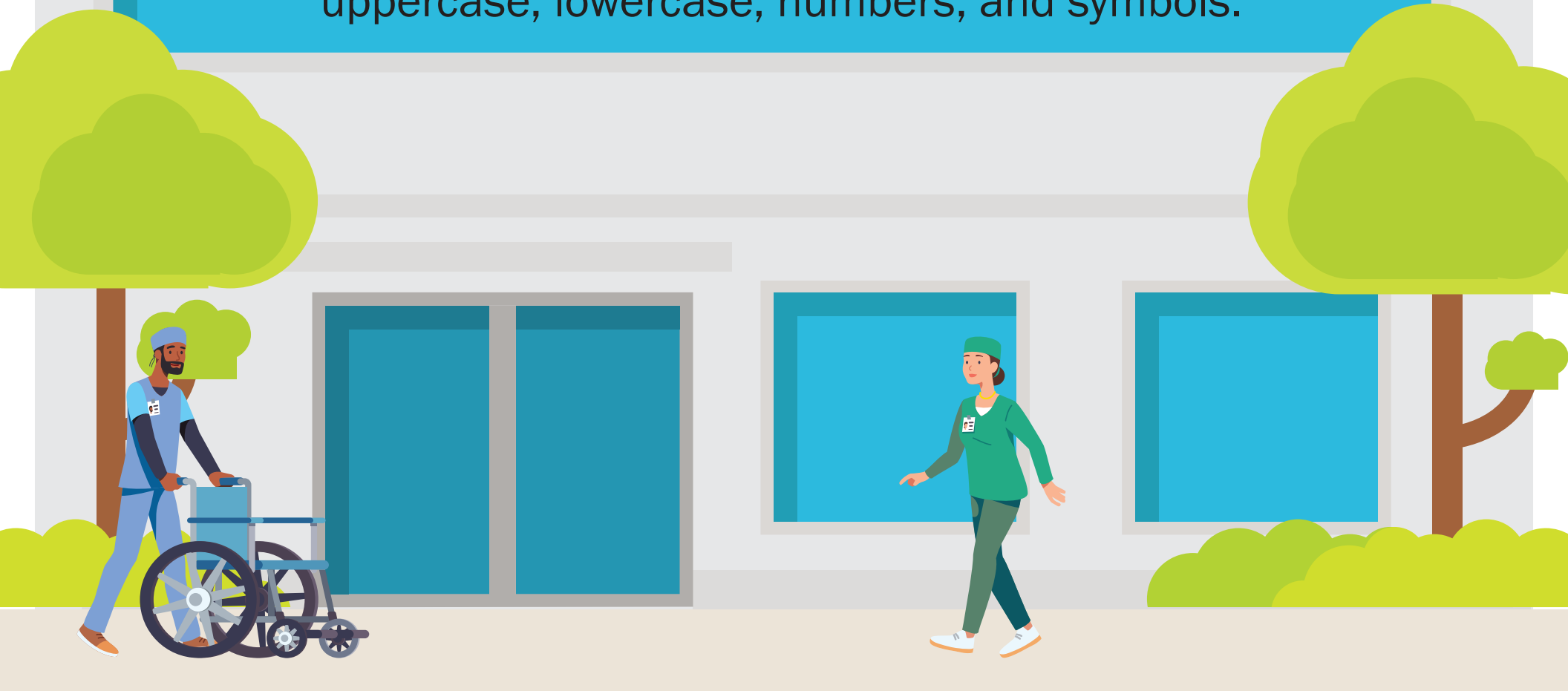




# Your Healthcare Facility's Name Is Not A Password



It is important to use strong passwords or a password phrase to protect patient data. As a best practice, passwords should be at least 16 characters long, randomly generated, unique, and include all four character types: uppercase, lowercase, numbers, and symbols.



**HHS 405(d)**  
Aligning Health Care  
Industry Security Approaches

**Cyber Care  
is Patient Care**

Cybersecurity Awareness Month

New message



# Do You See What I See?

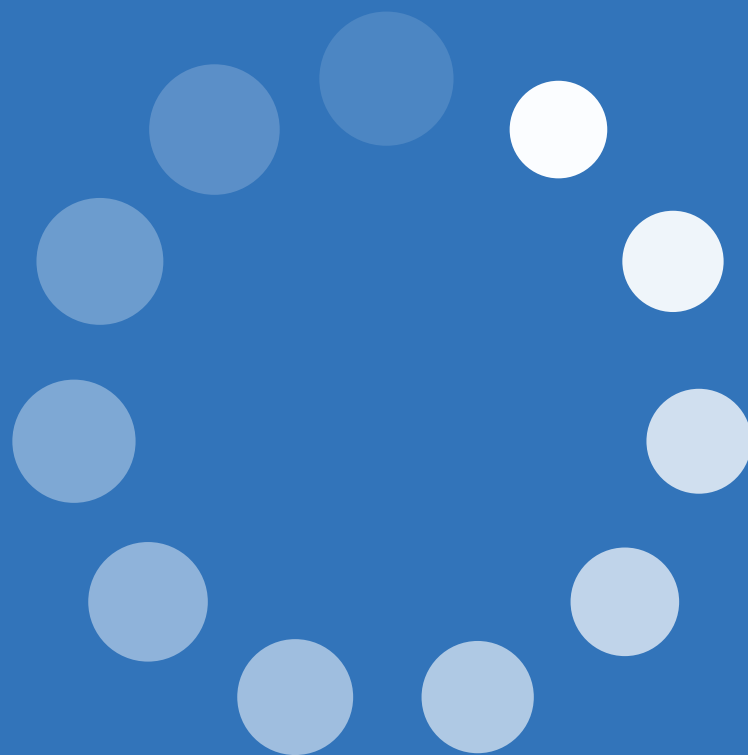
Look closely, do you know the sender? If you've ever seen a link that looks a little off or an email that asks for your personal information, it's likely a phishing scheme. Don't click on links or open attachments sent from an unknown source!



**HHS 405(d)**  
Aligning Health Care  
Industry Security Approaches

**Cyber Care  
is Patient Care**  
Cybersecurity Awareness Month

# Software Updates Provide Security Protection



Enable automatic updates on devices and software to ensure timely security patches are installed without having to take action. It is also important for all end users to update their software when prompted.



**HHS 405(d)**  
Aligning Health Care  
Industry Security Approaches

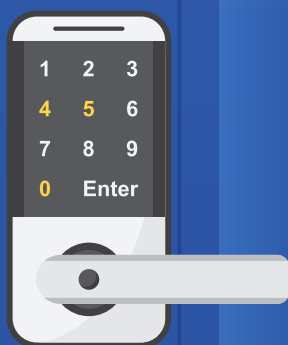
**Cyber Care  
is Patient Care**

Cybersecurity Awareness Month

# Two Locks Are Better Than One



In today's world you need more than a password to protect your organization and enabling MFA makes you significantly less likely to get hacked. Be sure to enable MFA on all appropriate accounts, especially your email systems, and use authentication apps or hardware tokens for even more added security.



**HHS 405(d)**  
Aligning Health Care  
Industry Security Approaches

**Cyber Care  
is Patient Care**

Cybersecurity Awareness Month