Training Bulletin Guidance—
Mobile Device Security is Essential to a Robust Cybersecurity Program

Trainer Notes

Mobile devices provide great value to organizations in the form of increased productivity. But the increase in use of mobile devices leads to more lost and stolen devices and potentially significant data breaches. The healthcare industry is particularly plagued with consequences of lost and stolen mobile devices. For example, the University of Texas MD Anderson Cancer Center just paid over $4,000,000 because of three separate data breaches involving the theft of an unencrypted laptop and the loss of two USB thumb drives containing the unencrypted protected health information of patients. There are effective ways to reduce the occurrence of lost and stolen mobile devices and the resulting negative business consequences.

Organizations should first implement a comprehensive mobile device and media policy which outlines the proper use and storage of mobile devices. If a policy is already in place, organizations should review it and make sure it is adequate. A device and media policy should be in **writing and communicated to all employees** including during new and refresher employee training. Employee training of good mobile device habits is critical.

Other actions include encrypting all mobile devices, never leaving unattended your mobile device in a public area, securing the device out of sight and in your trunk if the device must be left in the car, and never store a password with the mobile device or its case.

Talking Points for You and Your Employees

- Data breaches are not just hackers electronically accessing your computer networks.
- Review the tips provided on the following page.
- Go over your mobile device management policy with new and existing employees.
- Remind employees that cybersecurity is a team effort. Every employee counts, and participation is needed to maintain a good security posture.

CYBERSECURITY TRAINING BULLETIN

THE IMPORTANCE OF MOBILE DEVICE (LAPTOP) SECURITY

Lost and stolen laptops and mobile devices directly affect an organization's bottom line.

The cost of a lost or stolen device is far greater than just the price of the device. Other costs include the value of the data on the device, fines and penalties from regulators, the reputational harm of a potential data breach and more.

So - keeping your laptops and mobile devices secure is very important!

Use these tips to keep your laptops and mobile devices secure!

- Laptops should always be stored in secure areas.
- Never leave laptop bags unattended in airports or other public facilities, and always use the hotel safe to secure equipment when you're not in the room.
- When traveling, keep laptops in the trunk and out of sight (if they must be left in the car).
- When flying, do not put laptops in your checked bags - secure your laptop in your carry-on bag.
- Don't keep your laptop passwords with the laptop or its case.

What if my laptop is lost or stolen?

If any device you use for work (including your own devices like a smartphone or laptop) is lost or stolen, **IMMEDIATELY** contact your supervisor, IT department or other individual as specified in your organization's mobile device management policy.

Cybersecurity is a team effort. Every employee counts, and participation is needed to maintain a good security posture.