Click the link to view a video on

**Ensuring the Security of Electronic Health Records**

Adhere to these UTHealth policies

**Mobile Devices**
- If mobile devices are used to **access** University data, e-mail or confidential information, the mobile device must be authorized and use a “Secure profile” per the UTHealth Mobile Device Policy.
- All USBs and any other portable devices must be encrypted.
- Do not **store** confidential information on mobile devices.
- Confidential information should only be **stored** on UTHealth Highest Security Zone servers.

**Personally owned laptops/personal computers**
- Do not **store** University data or confidential information on personally owned laptops/personal computers regardless of the encryption status.
- Confidential information should only be **stored** on UTHealth Highest Security Zone servers.

While not all inclusive, we recommend these basic safeguards while you access UTHealth resources:

1. Do not share your password with anyone EVER!

2. Beware of Phishing e-mails. Do not click on e-mail links or reply to e-mails requesting your username and password.

3. Handle UTHealth data appropriately, especially on mobile devices and personally owned laptops and personal computers.

4. Ensure your device has anti-virus, anti-spyware and anti-malware installed and regularly updated.

5. Forward suspicious e-mail as an attachment to or contact IT Security if you have questions or concerns.

**IT Security**

its@uth.tmc.edu
713.486.2251