Empower Yourself to Protect Your Information

Your Health Information is Your Personal Property

What is your health information?
It can be any data about your medical history, current conditions and even include fitness activities.

Where is your health information located?
It can be in your health care provider's electronic health record, on your computer or mobile devices.

How is your health information protected?
If certain health care providers have your information, they must protect it under federal laws.
Only you can protect your health information under your control.

The Military Health System and the Defense Health Agency emphasize the value of personal health information. Know how to protect your health information and make safeguarding it a daily routine.

Make Health Fitness and Cyber Fitness a Daily Routine

Protect your personal health data when entering it into your fitness wearables, mobile devices, mobile apps and web sites, especially those with interactive tools that track and share your information.

Tips for your devices

- *Configure your device to be more secure – such as limiting the data the apps can access.*
- *Limit exposure of your mobile phone number.*
- *Carefully consider what information you want stored on the device.*
- *Maintain physical control of the device especially in public places.*
- *Disable interfaces that are not currently in use such as Bluetooth or Wi-Fi.*
- *Avoid using public Wi-Fi hotspots and unknown Wi-Fi networks.*
- *Delete all information stored on a device before you discard it or send it off for repair.*

Tips for your apps

- *Be selective in the apps you install and use on your mobile devices. Apps obtained via official app stores are usually more trustworthy than third party apps.*
- *When you grant permission for an app to access information on your device, you should be aware that some apps may be able to access your contacts, location, call logs, internet and calendar data, app usage and the device's unique IDs.*
- *Only store personal health information in apps provided by a Health Insurance Portability and Accountability Act (HIPAA) compliant organization.*

Protect and Connect

Protect your information when going online and using your mobile devices

- *Create strong passwords and change them often. Never share them.*
- *Use different passwords for systems or apps that store health care data.*
- *Use trusted virus and malware protection software.*

When You're Social, You're Global

Think carefully before posting anything on the internet that you don't want shared

- *Be aware your internet searches, website visits and postings can be tracked by others who want your information for their personal and financial gain.*
- *Consider using a fictitious name if you interact in a health-related chat room.*

EMPOWER YOURSELF TO PROTECT YOUR INFORMATION

Keep Your Health Information on Track

Protecting your health information is as important as safeguarding your financial information. Your health information can contain social security numbers, identification numbers and contact information. Someone could steal your personal information to purchase expensive pharmaceuticals, medical procedures and supplies, and you could receive the bill.

Protect yourself from health information fraud

- *Monitor your credit history frequently.*
- *Check your medical and insurance statements for accuracy. Compromised health records can go undetected for months.*
- *Develop a fraud protection plan for notifying providers and credit institutions if your information has been compromised.*

Share your personal and health information with extreme care

- *Validate the authenticity of a request for your medical information before you share it.*
- *Don't give out unnecessary information such as your driver's license or social security number.*
- *Avoid sharing your information over the phone unless you initiated the call.*
- *Never share sensitive information through an unsecured e-mail account or website.*
- *Use a secure messaging portal if it is available to exchange information.*

Store your health information wisely

- *If you store your health information online, know the website's privacy policy and service terms.*
- *If you download and store your health data on your computer or mobile device, keep your health data in password protected files or on external drives that can be disconnected from the internet.*

Don't Be a Victim of Phishing

Beware of identity thieves who trick you into sharing personal information through e-mail scams

- *Don't reply to e-mails or texts that request your personal or medical information. Reputable organizations provide a phone number and/or an official web site for sharing information securely.*
- *Don't open attachments or click on links contained in e-mails from an unknown source. One click can be enough to install and run malicious software on your computer.*
- *Use two e-mail accounts, one for health and financial information and the other for social media.*
- *Use different passwords for each account. This makes it harder for a would-be attacker to rely on one password to access all of your accounts.*

Using Public Wi-Fi? Use Caution.

Protect your information when using public Wi-Fi sites

- *Confirm your hotel and public Wi-Fi network ID and connection instructions.*
- *Take your computer offline if you suspect it was compromised.*
- *Use websites that start with "https:" so you know they are fully encrypted.*
- *Don't share personal health and financial information over a public Wi-Fi.*
- *Don't use mobile apps that contain your financial information.*
- *Only store personal health information in mobile apps provided by a Health Insurance Portability and Accountability Act (HIPAA) compliant organization.*

www.TRICARE.mil/cyberfit