West Virginia Executive Branch
Privacy Tip
This tip is brought to you by The Privacy Professor ® Rebecca Herold. Used with permission.

What is more valuable than money?

To a cybercriminal, medical data is 10 times more valuable than a credit card number.

Just as retailers and banks are closing security gaps to keep hackers from penetrating their systems, healthcare organizations, medical health device builders, and their vendors and contractors, must build in better privacy controls to keep health information secure. This is one of several calls to action Rebecca Herold is making in advance of this year's Data Privacy Day.

Consumers are becoming increasingly aware of the threat facing their health information. In a recent survey conducted by The Privacy Professor® more than a third of respondents said they are "not confident at all" their healthcare provider is appropriately safeguarding their patient information. That's likely due to news coverage of things like email phishing attacks and medical data breaches. However, not many people are thinking about the 'legitimate' ways their information is being shared by well-intentioned professionals, healthcare vendors and connected gadgets.

The 'Internet of Medical Things' is not on the radar of most Americans. In an increasingly connected society, where everything from your fitness band to your smart car are monitoring your body's function and performance, the risks are coming from many different places. It can be hard to keep track of the risks.

To open more eyes to the threats posed by the Internet of Medical Things, Rebecca Herold has developed an infographic (attached and linked here) enumerating some of the ways in which health data is collected and shared, often through unencrypted or insecure means. The infographic takes a look at the following threats and more:

- Wearables: 500 million users' health data at risk from unauthorized smartphones that can easily connect to unsecured fitness bands.
- Smart Cars: Connected car technologies communicate "total impairment scores" to insurance companies.
- WiFi Tracking: Frequencies allow humans to be seen behind walls and provide means for the detection of respiration and heart rates.
- X-Rays/Imaging: Connected medical equipment transmits patient data across the web, often without encryption.
- BYOD: Healthcare staff connect their unsecured personal devices to hospital networks, exposing patient data via vulnerable WiFi connections.
- Drug Pumps: Drug libraries open to hackers who can remotely set fatal doses.

The Privacy Professor® encourages all consumers to ask the healthcare entities and fitness tracker businesses with which they do business how their data is secured. Just as important, is reading and understanding the privacy policies that come with 'smart' gadgets and other connected technology.

All patients and consumers have the right to demand the collection, storage and sharing of their health, and other personal, information is as secure as possible.

Source: Rebecca Herold (a.k.a. The Privacy Professor), privacyguidance.com, rebeccaherold@rebeccaherold.com. Used with permission.

Note: Your agency/bureau/department/division may have specific requirements – always check your policies and procedures. If you have questions, contact your Privacy Officer.