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.

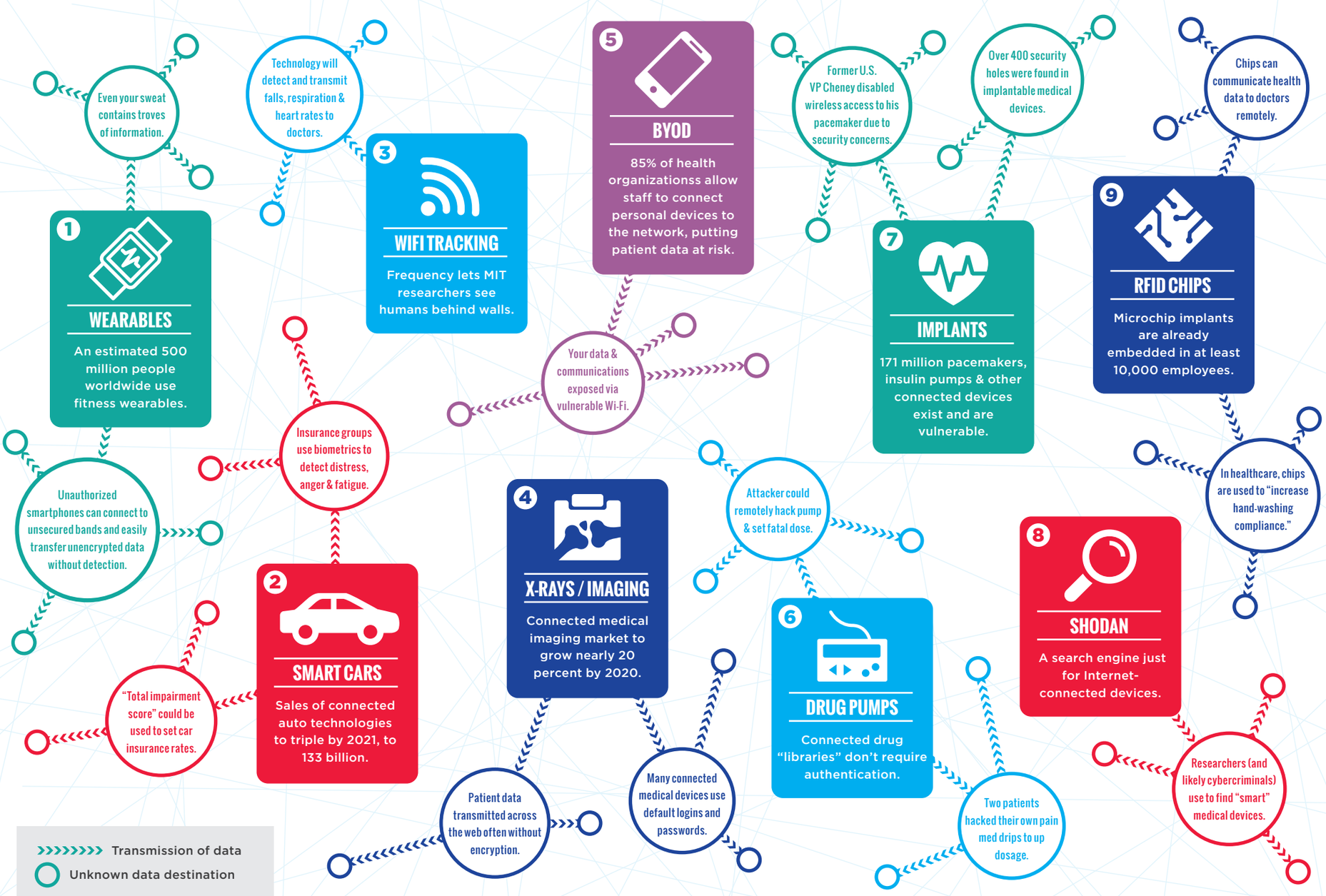
The Privacy Professor® encourages all consumers to ask the healthcare entities and fitness tracker businesses with which they do business how their data is secured. Just as important, is reading and understanding the privacy policies that come with 'smart' gadgets and other connected technology.

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.

WHO HAS YOUR HEALTH DATA?

When a cell divides, it makes a copy of its DNA. That copy must be verified perfect before the cell will split. Can we say the same about our health data, copied and shared millions of times by hundreds of medical devices, networks and systems?



Your body contains ONE HUNDRED TRILLION tiny cells.

That almost unfathomable number is nothing compared to the amount of health data your body generates. Scientists need a microscope to analyze your cells. Yet, an individual needs little more than a WiFi connection to access your medical data (which reports to be 10 times more valuable to a hacker than credit card info). As the Internet of Medical Things spawns the birth of more connected medical devices, privacy and security controls are vital to the wellness of all humans.

PRIVACY PROFESSOR™

SOURCES

Hackers hijacking medical devices to create backdoors in hospital networks http://www.computerworld.com/article/2932371/cybercrime-hacking/medjack-hackers-hijacking-medical-devices-to-create-backdoors-in-hospital-networks.html
Rising use of BYOD in healthcare increases security, privacy risks http://www.fiercemobileit.com/story/infographic-rising-use-byod-healthcare-increasing-security-privacy-risks/2015-05-13
Is Hacking Implanted Medical Devices the Next Big Cyber Crime? http://null-byte.wonderhowto.com/forum/is-hacking-implanted-medical-devices-next-big-cyber-crime-0149205/
Sweat Sensors Will Change How Wearables Track Your Health http://spectrum.ieee.org/biomedical/diagnostics/sweat-sensors-will-change-how-wearables-track-your-health
Will real-time health data for consumers add up to healthier living? http://www.pbs.org/newshour/bb/will-real-time-health-data-for-consumers-add-up-to-healthier-living/
Fitbit security slammed in tracker test http://www.wareable.com/wearable-tech/firm-tests-security-of-fitness-bands-and-finds-major-flaws-1290
Medical devices too prone to hackers, researchers warn http://www.washingtontimes.com/news/2015/aug/6/medical-devices-too-prone-hackers-researchers-warn/
Tech Trends for 2016: Real life cyborgs http://startups.co.uk/tech-trends-for-2016-real-life-cyborgs/
RFID in Health Care 2015 Report https://www.rfidjournal.com/purchase-access?type=Article&id=13812&r=%2Farticles%2Fview%3F13812
Hacker Can Send Fatal Does to Hospital Drug Pumps http://www.wired.com/2015/06/hackers-can-send-fatal-doses-hospital-drug-pumps/
State Farm Plans to Get Inside Your Head While You're Driving — and Put a Price on It https://www.nerdwallet.com/blog/insurance/state-farm-driver-emotions-price-car-insurance/
Connected Car Study 2015: Racing ahead with autonomous cars and digital innovation http://www.strategyand.pwc.com/reports/connected-car-2015-study
Wi-Fi technology can "see" people through walls https://www.youtube.com/watch?v=PnvcjKXo-AY
ABI Research Sees 17 Percent CAGR For Connected Medical Equipment https://satnews.com/story.php?number=1368014424
Testing wireless medical devices http://www.slideshare.net/NorthwestEMC/testing-wireless-medical-devices