NNEDV

# Connected Health & Medical Devices: Survivor Privacy Risks & Strategies

Many health and medical devices are now connected to the Internet, offering to help track information for the user, or even send that information to a doctor. Unfortunately, these devices and systems can provide yet another, highly invasive way that technology can be misused to monitor, harass, threaten, or harm a survivor. At the same time, they can also offer potential tools survivors can use to strategically increase their safety. There have already been examples where data from these devices was used as evidence in criminal cases.

## What is "IoT"?

The Internet of Things refers to devices connected to each other and to a device or app that can control them. These devices may be connected through the Internet, Bluetooth, or other means.

### *Consumer Electronics*

An increasing number of devices are marketed to help people get more active, lose weight, and to support a healthy lifestyle. The most common devices are step trackers and smart watches. Exercise machines now offer to connect to a mobile device to track and share information about the duration and intensity of a workout, as well as vital signs like heart rate. Athletic shoes can be connected as well, sharing information including location.

### *Medical Devices*

Newer devices for tracking vital signs collect, analyze, and share information, including blood pressure monitors and thermometers for tracking fertility. Medical equipment such as wheelchairs, pacemakers, or pill bottles, include the capability of tracking location or frequency of use and reporting that back to a doctor or medical facility.

*Big Data*

Information from connected devices is being fed into large sets of data held by companies and governments. These data sets may contain identifying, inaccurate, and potentially damaging information.

**Privacy and Safety Risks**

While everyone may face privacy risks from unauthorized access to the data from health and medical devices, survivors face specific risks to privacy and safety. Information about location, physical activity, vital signs, or habits could be misused to threaten or harm a survivor. Sensitive personal information could be shared publicly in an attempt to ruin a survivor's reputation. For example, usage data from connected sex toys used by survivors as part of healing from abuse, could be shared with an employer or others. Inadequate built-in security of devices, and the data they gather, raises concerns that the devices could be tracked, or even disabled remotely.

Additionally, the collection of this data may lead to risks to survivors' economic situations as insurance rates or employment are linked to health behaviors. Data from health devices may be combined with other data sets: as more people opt to have their DNA analyzed, this information could be matched with lifestyle and health information, or medical records related to abuse, negatively impacting a survivors' ability to seek affordable health care.

**Potential Benefits to Survivors**

Survivors with disabilities or those who face complex medical issues, have trouble remembering health-related tasks, or simply want to improve their health may all benefit from connected devices. The effects of trauma can hinder the ability to remember daily tasks, decrease motivation for physical activity, or impact heart rate and other vital signs. Connected devices could be part of a plan to improve wellbeing or track the impacts of trauma. The use of specific health and medical devices may help to lessen symptoms and illnesses that result from trauma or physical injury. All of these benefits may be undermined by a lack of privacy and

security, and so survivors and any health professionals they are working with should take these factors into account when selecting devices.

**Evidence**

Recent news stories have covered cases in which the data from health and medical devices has been used in criminal cases. Information about location, movement, and vital signs will likely be increasingly used to support or counter the version of events surrounding crimes. This same evidence may also be used in civil legal settings to support protection orders or family law matters. Evidence from connected health and medical devices may be stored on the device itself, on a mobile device, in a user's account, or on the server of a manufacturer or medical provider. In some cases, a survivor may have access to the data, and in other cases a subpoena or court order may be necessary to access the data.

**Questions About IoT Devices**

When considering connected health and medical devices, there are a few questions to consider. First, does that particular device truly need to be "smart" or "connected"? Do the benefits outweigh the risks? How secure is the device and the app that runs it? Are there features that allow the user to individualize and increase privacy and security?

**Strategies to Increase Privacy and Safety**

Steps to increase the privacy and safety include learning about the built-in security options of the device, turning it off when not in use, and changing the default passwords or other security settings. Ask doctors about using a device that is not connected to the Internet, or alternatives like keeping a handwritten log of the information that would otherwise be shared, or other ways of setting up reminders to take medication or exercise.

If a survivor suspects that a device is being misused, they can begin to document the incidents. Our technology abuse log is one way to document each occurrence. These logs can be helpful in revealing patterns, determining next steps, and may

potentially be useful in building a case if the survivor chooses to involve the legal system.

A survivor might also try to access evidence through the device, or the app or website that controls it. They can also try to reach out to the manufacturer to try to regain control over a device or the account associated with it. With these devices and others, it is also important to take steps to increase network and WiFi security. For more information, see our handout on WiFi security.


Supported by US DOJ-OVC Grant # 2016-TA-AX-K069. Opinions, findings, and conclusions or recommendations expressed are the authors and do not necessarily represent the views of DOJ.

This is one in a series of handouts describing the risks and potential benefits of IoT devices. We update our materials frequently. Please visit TechSafety.org for the latest version of this and other materials.