

High-tech drug infusion pumps in hospitals vulnerable to damage, hackers

March 21 2022, by Dennis Thompson



You've probably seen an infusion pump, even though the name might

make it sound like a mysterious piece of medical technology.

These devices govern the flow of IV medications and fluids into patients. They help deliver extra fluids to people in the emergency room, administer monoclonal antibodies to folks with COVID-19, and [pump](#) chemotherapy drugs to [cancer patients](#).

"If you're watching a television drama, they are the boxes next to the bedside. Tubing goes from a medication bag through the pump to the patient," said Erin Sparnon, senior engineering manager for device evaluation at the non-profit health care quality and safety group ECRI.

But the widespread usefulness of these ever-present devices has also made them a top technology hazard for U.S. hospitals, experts say.

Damaged [infusion](#) pumps can cause a patient to receive too much or too little medicine, potentially placing the lives of critically ill patients at risk. Plastic can crack, hinges can pinch, electronics can fail, batteries can die—and a patient can be placed in peril.

"There are over a million infusions running in the U.S. every day. The good news about that is the vast majority of them are just fine. The bad news is that a one in a million problem can happen every day," Sparnon said.

"That's why infusion pumps get a lot of attention, because they're ubiquitous. They're everywhere and they're used on critical patients for critical medications," Sparnon said. "We regularly get reports from health care settings where patients have been harmed due to pump damage."

Damaged infusion pumps placed number three on [ECRI's list of top 10 technology hazards for 2022](#), mainly due to the potential for something

to go mechanically wrong with them, Sparnon said.

But others have raised concerns that "smart" wi-fi-connected infusion pumps could be hacked and manipulated to harm patients.

Still, Sparnon said an infusion pump that's been manhandled or damaged in some way poses a much greater and more concrete safety risk than the possibility of a hacked pump.

"I know it sounds really cool, but there are no reports of patient harm due to a hack," Sparnon said. "I would put a lot more emphasis on the challenges of pumps being damaged, for sense of scale."

But earlier this month, Palo Alto Networks' computer security team Unit 42 [issued a report](#) noting that security gaps had been detected in about 150,000 infusion pumps, putting them at heightened risk of being compromised by attackers.

"There are a large number of known vulnerabilities that are specific to infusion pumps, specifically related to sensitive information leakage, unauthorized access and device denial of service," Unit 42 researcher Aveek Das said. "These vulnerabilities are well-documented, and based on our study we found one or more of these vulnerabilities affect 75% of the pumps we analyzed."

More infusion pumps, more chances for damage

Infusion pumps are not a new concern in health care safety.

Back in the mid-to-late 2000s, the U.S. Food and Drug Administration received about 56,000 reports of adverse events associated with the pumps, and 87 recalls were issued to address specific safety concerns.

What's more, [infusion pumps](#) have become more widely used in health care, pretty much anywhere IV fluids are administered.

"If you think about maybe even 40 years ago, infusion pumps were really only used for a certain subset of infusions," Sparnon said. "Most things were delivered just with a bag and a tube and a roller clamp."

As pumps have become more widely used, they have become more subject to everyday wear-and-tear, Sparnon said.

"It's not unusual for a 200-bed hospital to have hundreds of infusion pumps they're dealing with," Sparnon said. "Because there are so many pumps that are used for so many different therapies, they are wheeled around from room to room. They're a scarce resource in some facilities."

Pumps can be dinged by an elevator door, damaged by being dropped, or simply broken over time with heavy use, Sparnon said. And new ways to damage these pumps are cropping up all the time.

Take the pandemic, for example.

"There was a renewed emphasis on cleaning equipment between patients. This is good, because we want equipment to be cleaned between patients, to reduce the risk of transmitting germs from one patient to the next," Sparnon said.

"But in some cases, hospitals weren't following the instructions for use on how to clean the equipment, and might have been using wipes or solutions that weren't compatible with the equipment, or using incompatible cleaning methods—basically, scrubbing too hard," Sparnon explained.

The plastic in a pump damaged by aggressive cleaning or harsh sanitizers

can crack, causing fluids to drip into the electronic innards of the device. "Delicate electrical machinery doesn't like to have things dripping in on it," Sparnon noted.

"Twenty years ago, I don't think people were cleaning their infusion pumps all that often," Sparnon said. "As we've had an increasing emphasis on infection control, an unintended consequence of that was now we need to pay more attention to make sure that whatever cleaning processes we are doing are in accordance with what the supplier has tested out."

Those are just the everyday challenges placed on an infusion pump. The devices also continue to be subject to recall, for a number of different defects.

Das noted that the FDA issued seven recalls for infusion pumps or their components in 2021, and nine in 2020.

One of the most recent recalls occurred in December, when Baxter Healthcare [recalled more than 277,000 infusion devices](#) due to a faulty alarm system. The company had received three reports of patient deaths potentially linked to the flaw, as well as 51 reports of serious injuries.

'Smart' pumps carry hacking risk

As noted, Sparnon worries more about mechanical pump problems than the potential for the devices to be hacked. The ECRI report doesn't even mention hacking as a concern, focusing instead on damaged pumps.

"Smart" infusion pumps communicate via wi-fi to a dedicated server that supplies instructions on medication rates and other functions, Sparnon said.

"That's a pump speaking to its own server," Sparnon said. "Its own server then serves as a gateway to other information systems within the hospital, so it's not like the pump is hopping on the internet to find information or to receive programming."

But others, like Unit 42, believe hacking is a serious concern for smart infusion pumps.

The devices' shortcomings "included exposure to one or more of some 40 known cybersecurity vulnerabilities" or alerts related to "some 70 other types of known security shortcomings" for internet-connected devices, the report said.

The vulnerabilities detected by Unit 42 allowed for potential leakage of [sensitive patient data](#). The group also noted a number of security alerts coming from the pumps they analyzed, including login attempts using default credentials from the manufacturer.

"While some of these vulnerabilities and alerts may be impractical for attackers to take advantage of unless physically present in an organization, all represent a potential risk to the general security of health care organizations and the safety of patients—particularly in situations in which threat actors may be motivated to put extra resources into attacking a target," the security researchers concluded.

"Having devices compromised by malicious actors has the potential to impact patient safety and disrupt hospital operations," Das said.

"For example, a denial of service attack where an attacker sends specifically crafted network traffic to an [infusion pump](#) can cause the pump to be unresponsive," Das said. "In addition, certain vulnerabilities could potentially be exploited to intercept clear-text communications between a pump and its server, thereby leaking sensitive patient

information."

Hospitals need to shore up computer security

To protect against hacking, Unit 42 recommends that health care computer systems use "zero trust" networks that require continual verification.

"That way, compromised pumps are immediately detected, which enables clinicians to swap them out and prevent malware from spreading across hospital networks," Das said.

Sparnon believes efforts by groups like Unit 42 are making infusion pumps safer from hacking.

"Hacking of infusion pumps happens in academic settings and that's good, because it helps suppliers figure out how to properly secure their servers," Sparnon said.

As far as the more widespread problem of physically damaged infusion pumps, Sparnon believes clinical staff can play a leading role in protecting patients from faulty devices.

"Don't use a pump if it has visible damage or if any part of the setup seems abnormal, like the door is hard to close or there's air in part of the infusion set where you wouldn't expect to see air," Sparnon said.

"If you see an alarm on the pump that you don't really understand, in that case you should take that pump out of use and put a tag on it noting what you saw. You need to describe the problem because then you need to send it down to clinical engineering, the department within the hospital that cares for equipment and makes sure it's ready for use," Sparnon said.

"They might find a particular part on their infusion pumps is wearing out too quick. They might find that a particular alarm keeps getting set off too often. Those trends can really be helpful for the hospital to work both internally and with ECRI and with their supplier to figure out what's going on," she explained.

"I would consider it like almost a horse race," Sparnon said of the need to remain vigilant regarding infusion pumps. "Over time, the problems change. We solve the problems, and then new ones emerge."

More information: The U.S. Food and Drug Administration has more about [infusion pumps](#).

Copyright © 2021 [HealthDay](#). All rights reserved.

Citation: High-tech drug infusion pumps in hospitals vulnerable to damage, hackers (2022, March 21) retrieved 27 April 2024 from <https://medicalxpress.com/news/2022-03-high-tech-drug-infusion-hospitals-vulnerable.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--