HUME CENTER FOR NATIONAL SECURITY AND TECHNOLOGY
VIRGINIA TECH

August, 2020

Whitepaper

An Invisible Insider Threat: The Risks of Implanted Medical Devices in Secure Spaces

Zoe Chen, Paul O'Donnell, Eric Ottman, Steven Trieu, Dr. Alan J. Michaels
Hume Center for National Security and Technology
Virginia Polytechnic Institute and State University

A growing number of IC employees rely on implanted medical devices—insulin pumps, pacemakers, and the like—with embedded memory and data processing, communication, and adaptive capabilities that pose a security threat to the community's secure work spaces. Because the technology in these smart devices has far outpaced current security directives, new security-in-depth technical and policy mitigations are needed to support the use of medically critical technology while safeguarding the IC's secure spaces.

This whitepaper explores the question: "Does the IC need to update policies aimed at mitigating the risks associated with the presence in secure IC workspaces of implanted medical devices (IMDs), such as pacemakers, insulin pumps, cochlear implants, and neurostimulators?" These devices are permanently or semi-permanently inserted to replace or assist bodily functions and maintain patient health, which makes them nearly impossible to remove, disable, or pause while in a secure facility. IMDs increasingly include smart features enabling them to connect wirelessly to external equipment so patients and physicians can monitor their effectiveness in real time. Although this wireless connectivity clearly provides critical health benefits for IC employees, it also creates a potential unwitting insider threat to national security. Introducing smart IMDs into secure spaces increases the likelihood that users unknowingly release protected information to unauthorized, external entities—the most pervasive being identifying a user's GPS-derived presence in a secure facility. Two-way communications (e.g., Bluetooth) and voice-activated user interaction present even greater risks to classified information. Current IC security policies are largely unprepared to address the unavoidable risks posed by these devices. This paper proposes a family of technical mitigations aimed at helping balance workforce protections and national security.

Motivation

Policy addressing these IMDs, which may be questionably extended also to wearable medical devices like fitness trackers, is defined in the Office of the Director of National Intelligence's ICD-705, which has undergone three revisions in the last decade, offering no guidance on medical devices in 2012 [1], updated to include a footnote exempting medical devices from the portable electronic device (PED) restrictions in 2015 [2], and recently adding a paragraph delegating cognizance and responsibility to the facility owner in 2017 [3]. At the same time as ICD-705, which is primarily concerned with protecting classified information within a secure facility, employers have a duty to ensure they provide reasonable accommodations to the workforce to perform their jobs when possessing a physical disability or related condition; such protections are codified in the Rehabilitation Act of 1973 [4], the Americans with Disabilities Act [5], and reiterated explicitly by IC policy guidance 110.1 [6]. IMDs and other medical devices can easily be argued to fit within these protections.

Our observations for the practical implementations of these potentially conflicting guidelines, however, are that the HR-focused protections dominate, resulting in policy exemptions (without any technical mitigations) for individual hosting IMDs. As these medical devices rapidly inherit the capabilities of other connected Internet of Things (IoT) devices, the associated risk levels are increasing sufficiently that we propose the adoption of updated policy and technical mitigations to help manage the risks, simultaneously addressing the concerns of workforce protections and national security. Taking into account current PED mitigations, such as leaving most devices in metal boxes outside the facility, and increasing prevalence of IMD waivers, we arrive at a residual facility risk shown in Figure 1, using the qualitative PED risk guidance defined in ICD-705.

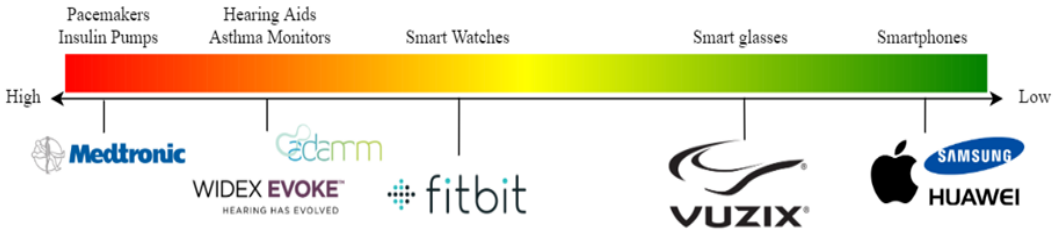


Figure 1. Residual security risks associated with various PED classes, accounting for practical implementation of secure facility policies

IMDs: A Growing Presence in the IC Workforce

The use of IMDs within the United States has become commonplace and, with continued technological innovation, almost certainly will become even more pervasive. According to the National Institutes of Health, for example, the number of adults in the United States who received cochlear implants to improve hearing rose from 42,600 in 2010 to 58,000 in 2012—a 36-percent jump in just 2 years [7]. Pacemaker implants similarly rose, from 188,700 people in 2009 to at least 250,000 annually in 2017 [8]. This suggests that about 0.02 percent of the adult U.S. population had cochlear implants in 2010 and just under 0.64 percent had pacemakers. Related research estimates that 7 percent of diabetes patients used insulin pumps in 2010, or about 0.71 percent of the population [9,10], and that 0.83 percent of the population has hip implants, which are beginning to incorporate wireless capabilities

[11]. The marked increase in implantation rates since 2010 and the increasing wireless capabilities of those implants suggest even greater percentages of the population with IMDs and even higher security risks during the past decade.

The IC cannot meet security requirements simply by refusing to employ people who rely on IMDs. All Federal facilities must comply with the Rehabilitation Act of 1973, which prohibits discrimination against employees with smart IMDs, and other U.S. laws, such as the Americans with Disabilities Act and the Health Insurance Portability and Accountability Act (HIPAA), ensure individuals' health records remain private. No statistics exist on the number of IMDs among the roughly 4.3 million people—about 1.4 percent of the U.S. working age population—who had active U.S. security clearances in 2010 [12]. Figure 2 shows our estimates for the four most common types of IMD, extrapolated from the percentage of patients with these devices within the overall population. Given the increase in annual implants since 2010 and the aging national security workforce, it is safe to assume these numbers have only grown.

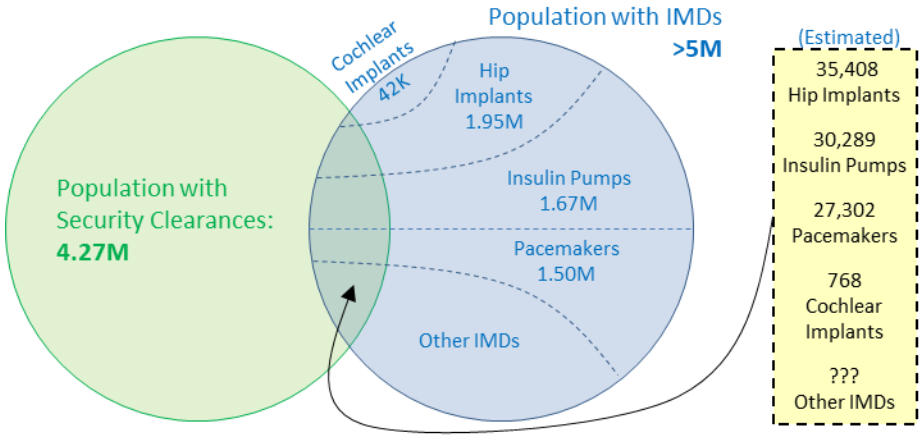


Figure 2. Estimate of cleared workers with IMDs.

Risk to the IC Workplace

All of these IMDs provide bona fide health benefits, and, unlike cell phones, fitness trackers, and other personal electronic devices (PEDs), they are rarely detachable or easily deactivated upon entering a secure facility. Current security policies rate these devices as either low, medium, or high risk [3].

- Low-risk devices cannot record or transmit data.
- Medium-risk devices are those whose ability to transmit or record data can be mitigated to acceptable levels.
- High-risk devices defy even complex or extensive mitigation efforts.

Receive-only GPS falls into the lowest risk category because its location data does not give out much more information than can be observed from watching the user's pattern of life, although GPS is easier to access. Reliance on a data server presents a medium-low risk. A device like the Widex Evoke hearing aid, for example, which works with a person's smartphone to customize how the hearing aid processes sounds, has limited functionality while in a secure facility if cloud access is prevented. When allowed cloud access, however, the Evoke is capable of machine learning—using cloud-stored data from multiple users and devices to develop better sound management [13].

Figure 3. Common device capabilities ranked on level of risk they pose to the facility

Medium- and high-risk devices are not allowed in secure facilities without prescribed precautions, if at all. Most IMDs fall into the medium- or high-risk categories because they are smart devices that transmit data to healthcare providers through connections with mobile devices and networks. The greatest security concerns within these devices are their transducers—the microphones, cameras, and other sensors that convert information from the environment into signals and data—because transducers open the possibility of using the device to illicitly remove information from a secure environment. The Cochlear and ReSound bimodal hearing solution, for example, has an app that can alter settings for devices and uses Internet connectivity to track statistics and metrics [14,15]. Similarly, the Medtronix MiniMed series automated insulin pumps use Bluetooth connections to transfer data to a user's smartphone, where it can be stored for as long as 90 days [16]. ADAMM is a wearable, flexible, and waterproof device worn on the chest to monitor heartbeat, temperature, and respiration to predict asthma attacks based on common precursor symptoms [17]. ADAMM transmits the collected data to the user's smartphone via Bluetooth. Almost all of these apps include GPS trackers that are accustomed to intermittent connectivity.

The most prevalent form of two-way communication in IMDs is Bluetooth—which, along with other Internet of Things protocols, possesses many known exploits [18]. Open-source code also poses a risk because it can be easily uploaded onto IMDs and allows malicious actors to manipulate device functionalities or exploit any backdoors; such exploits could even be used as part of socially engineered coercion attacks. Open-source IMDs are mainly DIY medical devices, where users wished for more support and economically feasible adjustments [19,20]. Some are in the process of gaining FDA approval. However helpful the device may be, open-source code is especially troublesome when the device has transducers and two-way communication. Moreover, few IMDs are made in the United States or can boast a trusted supply chain.

Potential Compromises and Recommendations

So how can information and privacy be protected while maintaining the health and safety of the IMD user?

Reasonable guidelines can be established to address the often contradictory goals of meeting IMD users' medical needs, while safeguarding classified and other sensitive information. These consist of technical mitigations, policy modifications, and acceptable exclusions from working within the secure facilities when mitigations are infeasible. Some guidelines to consider include:

- **Whitelisting:** Pre-approving a set list of IMDs would facilitate access to secure areas for employees. It would not prevent devices from being tampered with once approved and, unless consistent across IC agencies, might limit employees' access to other facilities. Some PEDs, even Bluetooth-enabled fitness trackers, are whitelisted in some facilities despite ease of spoofing.

- **Random Inspections:** Requiring Government-approved devices to undergo random inspections would identify those devices that have been compromised or users abusing information. For IMDs with a mobile interface, random inspections could ensure original software is not compromised, transducers are properly configured, and two-way communications only pair to trusted sources. Doing a baseline examination of IMD settings during the pre-approval process would provide inspectors with documentation to determine later if the settings or functions of an IMD have been altered or removed. Such inspections would probably require proprietary information from non-U.S.-based manufacturers.
- **Ferromagnetic Detection:** Using these detectors to identify implants or other foreign devices could ensure only whitelisted devices are being used. A 2018 Mayo Clinic study found that ferromagnetic detection systems (FMDS) accurately classified 34 different styles of cardiac pacemakers with 99.6-percent accuracy.
- **Zeroization:** Inspecting and clearing data from the device before it leaves the secure space would ensure information security when disabling the device's recording or storage capabilities is difficult. However, establishing safe and secure ways of deleting information is likely to be difficult for devices embedded in individuals.
- **Physical Signal Attenuation:** Requiring IMD users to shield the device in a Faraday cage while in the secure facility is one of the simplest safeguards, although many users are likely to find the foil shields cumbersome in practice. Most devices operate in the 2.4 GHz ISM band, which naturally has high signal attenuation due to H_2O absorption characteristics.
- **Administrative Software:** Developing code that would use a generated password to disable sensitive functions or override *connected* functionalities of the implant could put the device into an airplane-mode-like setting that could be managed by the secure facility.
- **AP Spoofing:** Hijacking the IMD's two-way communications to prevent normal two-way communication links could contain information spills, although the technique may erode IMD processing, battery consumption, and other core functions.

Although zeroization on its own provides the most security and is a commonly accepted practice for devices like test equipment in a secure facility, policy supplementations are recommended for IMDs because the risks are associated with human health, not simply with equipment. Implementing a physical inspection into the zeroization process at the end of the workday will help to compare stored values and ensure unwitting tampering has not occurred. Although not required, incorporating a third-party detection method like an FMDS will help to deter and prevent unauthorized devices from entering any secure area. Other mitigation methods may be used with the facility manager or accrediting officer approval, but thorough analysis of the IMD's capabilities should be the determining factor on the mitigation level, considering the residual risk level after chosen mitigations are put in place.

A summary of our recommended mitigations, along with qualitative rankings of risks to user and benefits to security posture are shown in Figure 4. Note that a mitigation is optimal when it presents little risk to the host and maximum benefit to protecting security – we recognize that this is not an easy problem, finding those in the highlight region to be the most practically implemented mitigations.

The Security and Health Trade-offs of Specific Mitigation Techniques

(1) **Random Physical Inspections** are similar to ICD-705 policy on government provided devices. Poses a low risk to the user; however, without sufficient knowledge on the specific device, difficult to catch the unauthorized extraction of data.

(2) **Ferromagnetic Detection Systems** may help identify smart devices before they enter any secure area, leading to facility manager decision whether or not to admit the individual. These systems do not prevent data extraction, only the detection of the physical device.

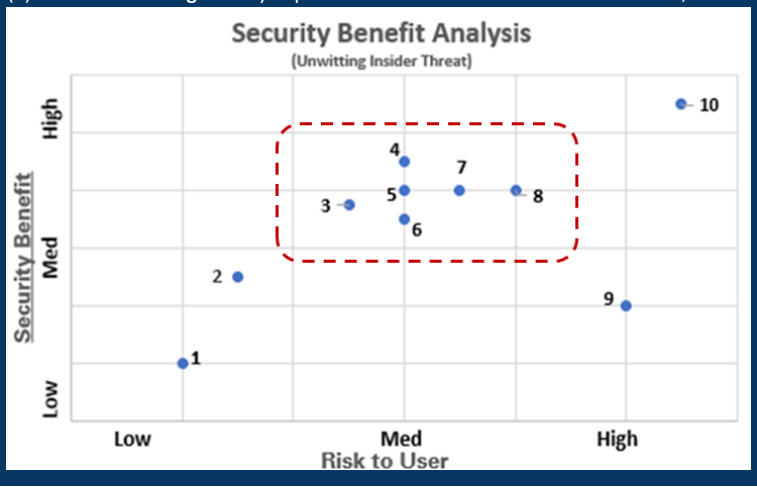
(3) **Radio Frequency (RF) Shielding Apparel** could be a foil vest that blocks communication with the IMD. This proposed vest would be worn by the host upon entering the facility. Signal leakage is still a concern.

(4) **Zeroization** is a safe method, but requires knowledge of the device and settings. All sensor data collected inside the SCIF must be removed to ensure protections. Because of this, a greater risk is imposed upon the user, because stored settings or essential functions may be disrupted.

(5) **Password Activated Software** is an administrator controlled software that takes over control of the device and limits suspect functions until a password is entered. This one-time use password would be provided to the employee after they have left the secure area.

(6) **Temporarily Muting Transducers** ensures valuable data cannot be recorded and stored. Users with cochlear implants would lose functionality as well as other similar styles of implants, many of whose residual capabilities impair human health.

(7) **Personal Jamming** actively impairs the communication or sensor functions, much like an audio white noise generator.



(8) **General Signal Jamming/AP Spoofing** hijacks Bluetooth, WiFi, and other commercial signals, preventing communication to third parties. This proves beneficial as no privacy laws are violated, yet could result in battery draws or other unintended effects to the medical device.

(9) **Tracking/RF Fingerprint** technologies mark an individual and monitor location and possibly record any signals. Such a technique likely violates privacy/HIPAA laws.

(10) **Denying Entry** completely eliminates the risk of data extraction, however the user would not be permitted to conduct any work within the area. While denial provides security, it fails to meet the practical needs of our ageing workforce.

Figure 4. Summary of technical mitigations with qualitative risks to individuals and benefits to national security.

Conclusion

The U.S. national security apparatus faces a constant challenge to balance information security and the quality of life of IMD-dependent employees. Rapidly changing technology and an ever-present need for balance between security and employee quality of life pose a constant challenge for the U.S. Government and businesses in the national security, military-industrial, and corporate sectors. In the case of smart IMDs and similar devices, emerging technology often does not fit within the scope of current U.S. policies and guidelines and can create challenges for employees of government agencies and contractors who require IMDs to maintain their health and job performance. In particular, smart IMDs are not specifically named in the guiding policy within Tech Spec 705, and thus abiding by the protections granted to individuals with disabilities in ICPG 110.1 leads to the introduction of high risk PEDs into our facilities. Note that this policy guidance has evolved over time as well, so there is clearly a recognition of the increasing threat level. However, even if PED guidance was updated to include IMDs, new mitigations methods are necessary to reduce the risk level of certain IMDs to acceptable levels. Based on analysis of the benefits and risks associated with various mitigation methods, the best means for maintaining information security and employee privacy include, but are not limited to, physical shielding, disabling certain IMD functions, zeroization, and the creation of admin software to enforce secure modes. The necessary policy framework and technology to achieve the aims of information security and employee privacy and comfort currently exist but should be amended and implemented accordingly to keep up with the changing needs and technology in secure spaces.

References

[1] *Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities*, National Counterintelligence and Security Center, Office of the Director of National Intelligence, v1.2, Apr 2012.
[2] *Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities*, National Counterintelligence and Security Center, Office of the Director of National Intelligence, v1.3, Sep 2015.
[3] *Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities*, National Counterintelligence and Security Center, Office of the Director of National Intelligence, v1.4, Sep 2017.
[4] *Rehabilitation Act of 1973*, 29 U.S.C. § 701 (9/26/1973).
[5] *Americans With Disabilities Act of 1990*, Pub. L. No. 101-336, 104 Stat.
[6] *Intelligence Community Policy Guidance 110.1: Employment of Individuals with Disabilities*, ODNI, Feb 2019.
[7] *Cochlear Implants*, National Institute of Deafness and Other Communication Disorders, June 2018.
[8] Skevos Sideris, et al., *Leadless Cardiac Pacemakers: Current Status of a Modern Approach in Pacing*, Hellenic Journal of Cardiology, no. 6 (Dec 2017).
[9] *Number of Americans with Diabetes Projected To Double or Triple by 2050*, Centers for Disease Control and Prevention, October 22, 2010.
[10] *Proportion of Insulin Dependent Diabetes Patients in the U.S. Using a Pump 2010*, Statista, July 2014.
[11] J. B. van Gaalen, et al., *Versatile Smart Hip Implant Technology Using 3D Metal Printing*, 2016 IEEE International Symposium on Circuits and Systems, May 22-25, 2016.
[12] *Annual Intelligence Authorization Act Report on Security Clearance Determinations For Fiscal Year 2010*, ODNI, Sep 2011.
[13] Widex Evoke–The World's First Smart Hearing Aid, Widex, accessed March 4, 2020,.
[14] Cochlear-Bimodal-Hearing-Solution, ReSound, accessed March 4, 2020.
[15] Nucleus Hearing Implant Smartphone Compatibility: Cochlear Americas, Cochlear, accessed March 4, 2020.
[16] 3 Ways to Get Started, MiniMed 670G Insulin Pump System, Medtronic, accessed March 27, 2020.
[17] Minhee Kang et al., *Recent Patient Health Monitoring Platforms Incorporating Internet of Things-Enabled Smart Devices*," *International Neurourology Journal* 22, no. 2 (July 31, 2018): 76–82.
[18] Y. Zou et al., A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends, *Proceedings of the IEEE* 104, no. 9 (September 2016): 1727–65.
[19] Nick Oliver et al., Open Source Automated Insulin Delivery: Addressing the Challenge, *NPJ Digital Medicine* 2, no 124 (December 11, 2019).
[20] Carmela De Maria et al., The UBORA E-Infrastructure for Open Source Innovation in Medical Technology, in *IFMBE Proceedings 76: XV Mediterranean Conference on Medical and Biological Engineering and Computing–MEDICON 2019*, ed. J. Henriques, N. Neves, and P. de Carvalho.