CYBERSECURITY IN MEDICAL DEVICES

Cybersecurity continues to gain attention as advancements in smart medical devices and platforms are made, and more providers opt for the use of connected medical devices. Beyond the technology itself, what makes the landscape more challenging to navigate is a multitude of guidelines, specifications, and standards set forth by various entities, including government, private, and hybrids of the two regarding cybersecurity practices for medical devices.

In addition to the U.S. regulatory landscape, there are also the international requirements, for example, Health Canada guidance on premarket requirements for medical device cybersecurity (2019)\(^1\), the Australia Therapeutic Goods Administration (TGA) medical device cybersecurity guidance for industry (2019)\(^2\), and the European Medical Devices Regulation (MDR)\(^3\) and In-vitro Diagnostic Medical Devices Regulation (IVDR)\(^4\).

It is important to note that both U.S. and international cyber security-specific requirements are in addition to other regulations dealing with protecting or processing of personal data stored in medical devices. For example, at the E.U. level, in addition to the MDR/IVDR regulations, the NIS Directive (E.U.) 2016/1148\(^5\) and the General Data Protection Regulation (E.U.) 2016/679 (GDPR)\(^6\), and the E.U. Cybersecurity Act (Regulation (E.U.) 2019/881)\(^7\), are also relevant to medical devices.

The key U.S. federal agencies, the Food and Drug Administration (FDA), Office of the National Coordinator for Health I.T. (ONC), and the Federal Communications Commission (FCC), each have unique responsibilities in the health I.T. arena and are working together on strategies and recommendations for an appropriate, risk-based regulatory framework.

THE FDA

The Food and Drug Administration (FDA) has issued several guidance documents over the past few years specific to cybersecurity considerations:\(^8\)

- Guidance to Industry: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software (January 2005)
- Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices (May 2005)
- Final Guidance on Postmarket Management of Cybersecurity in Medical Devices (December 2016)
  - Focusing on post-market management program for medical devices that includes the monitoring, identification and resolution of any identified cybersecurity vulnerabilities.
- Draft Guidance on Content of Premarket Submissions for Management of Cybersecurity in Medical Devices (October 2018)
  - Focusing on cybersecurity considerations that medical device developers and manufacturers should consider during the initial design and development phases for new medical devices.

While the FDA publications are guidelines, medical device manufacturers must comply with other federal regulations such as quality system regulations (QSRs)\(^9\), which require medical device manufacturers to address all risks, including cybersecurity risk. The FDA’s pre- and post- market cybersecurity guidances provide recommendations for meeting QSRs.
These guidances are not creating new classes of regulated products, or even reclassifying any products that have already been regulated. Instead, they apply to medical devices and in vitro diagnostic products (IVD) that include software (including firmware) or programmable logic ("Software in a Medical Device or SIMD) and "Software as a Medical Device" (SaMD). Software functions that meet the definition of a device may be deployed on mobile platforms ("mobile medical app"), other general-purpose computing platforms, or in the function or control of a hardware device.

The FDA also works closely with several federal government agencies, including the U.S. Department of Homeland Security (DHS), members of the private sector, medical device manufacturers, health care delivery organizations, security researchers, and end-users.

Exemplary sources of cybersecurity guidance in U.S. include:

- FDA Premarket and Postmarket Guidance
- NIST Framework for Improving Critical Infrastructure Cybersecurity
  - Identify, protect, detect, respond, recover
- HHS/HIPAA Security Rule\(^{10}\)
  - Recently released Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients
- FTC - Start with Security: A Guide for Business\(^{11}\)
- DOJ guidance\(^{12}\)
- State AGs (e.g., California\(^{13}\)
- SEC guidance on public company cybersecurity disclosures\(^{14}\)
- Certifications/standard-setting bodies (e.g., ISO\(^{15}\))

To mitigate cybersecurity risks, the FDA provides that Medical device manufacturers (MDMs) and health care delivery organizations (HDOs) should take steps to ensure appropriate safeguards are in place and states:

- Medical device manufacturers (MDMs) are responsible for remaining vigilant about identifying risks and hazards associated with their medical devices, including risks related to cybersecurity.
- Health care delivery organizations (HDOs) should evaluate their network security and protect their hospital systems.
- Both MDMs and HDOs are responsible for putting appropriate mitigations in place to address patient safety risks and ensure proper device performance.

The FDA is also a participant in the International Medical Device Regulators Forum (IMDRF)\(^{16}\), a voluntary consortium of national regulators representing major medical device markets around the world working to “accelerate international medical device regulatory harmonization and convergence.”

To help harmonize the global regulatory frameworks, the IMDRF provides: (1) a single audit program (MDSAP) which provides a common set of requirements for the conduct of regulatory audits of device manufacturers’ quality systems; and (2) a draft guidance, "Essential Principles of Safety and Performance of Medical Devices and IVD Medical Devices," addressing cybersecurity risks.\(^ {17}\)

**THE HSCC**

The Healthcare and Public Health Sector Coordinating Council (HSCC)\(^ {18}\) is a private-public partnership – made up of the Food and Drug Administration (FDA), Cerner, Mayo Clinic, and others, with oversight
from the Department of Homeland Security (DHS). The HSCC Joint Cybersecurity Working Group (JCWG) is a standing working group of the HSCC, composed of more than 200 industry and government organizations working together to develop strategies to address emerging and ongoing cybersecurity challenges to the health sector.\(^\text{15}\) The Medical Device and Health I.T. Joint Security Plan (JSP), published in January 2019, is neither a regulatory document nor a standard.\(^\text{20}\) It is a voluntary framework that includes associated plans and templates for use throughout the lifecycle of medical devices and health I.T.

The JSP is a complete product lifecycle reference guide to developing, deploying, and supporting cyber-secure technology solutions in the healthcare environment.

The JSP framework is designed around 4 key themes:

- **Design Control:** Building medical technology with cybersecurity standards and testing
- **Complaint Handling:** Preparing and managing deployed medical technology cybersecurity
- **Risk Management:** Assessing and responding to cybersecurity issues and events throughout the life cycle of medical technology
- **Maturity Evaluation:** Measuring and tracking the progress of a cybersecurity program for medical technology

**THE ONC**

The Office of the National Coordinator for Health Information Technology (ONC) is the principal federal entity charged with coordination of nationwide efforts to implement and use the most advanced health information technology and the electronic exchange of health information.\(^\text{21}\)

Health information technology, or health I.T., is defined by the ONC as "hardware, software, integrated technologies or related licenses, intellectual property, upgrades, or packaged solutions sold as services that are designed for or support the use by health care entities or patients for the electronic creation, maintenance, access, or exchange of health information."

The 2019 Interoperability Standards Advisory (ISA) process, represents the model by which ONC will coordinate the identification, assessment, and public awareness of interoperability standards and implementation specifications that can be used by the U.S. healthcare industry to address specific interoperability needs including, but not limited to, interoperability for clinical, public health, and research purposes.\(^\text{22}\)

While the ISA itself is a non-binding document and meant to be advisory in nature, standards and implementation specifications listed in the ISA may be considered for rulemaking or other Federal requirements. However, those decisions would be made on a case-by-case basis by the administering organization.

One application of the ISA is to the electronic health records (EHR), now widely used in physician practices, hospitals, and health systems across the U.S. As a result, the federal government and the private sector have focused on improving interoperability—the secure exchange of electronic health
information with, and use of electronic health information from, other health I.T. systems without special effort on the part of the user.

The Department of Health and Human Services, led by the ONC, released the draft 2020-2025 Federal Health I.T. Strategic Plan in January 2020.

The draft ONC 2020-2025 strategic plan has 4 primary goals, each goal having several objectives.23

For example, Objective 4d of Goal 4, focuses on the Promotion of secure health information that protects patient privacy, provides on the following strategies:

- **Integrate privacy and security considerations into the design and use of health IT** to promote a culture of privacy and security and protect individual- and population-level data from cybersecurity attacks, fraud, misuse, and other harms.
- **Implement privacy and security mechanisms as appropriate to the sensitivity of the data** to help protect individuals’ health data, including multi-factor authentication and encryption embedded in APIs and other technologies.
- **Increase patient understanding and control over their data** so they can make informed decisions about data exchange and secondary uses of their data.
- **Provide guidance and technical assistance on policies and regulations** at the federal, state, and tribal level that pertain to the secure exchange of health information and enforce such rules.
SO, WHERE DOES THIS ALL LEADS?

FDA recommends that device developers and manufacturers model their cybersecurity efforts, for medical devices around the five key functions identified in the NIST Cyber Security Framework:24

<table>
<thead>
<tr>
<th>Identify</th>
<th>Develop the organizational understanding to identify and manage cybersecurity risks to systems, assets, data and capabilities, based on the findings of a comprehensive risk management assessment consistent with the unique requirements of the organization.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protect</td>
<td>Develop and implement the appropriate safeguards to ensure delivery of essential services, and to limit or contain the impact of a potential cyberattack.</td>
</tr>
<tr>
<td>Detect</td>
<td>Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event, such as continuous security monitoring and detection processes.</td>
</tr>
<tr>
<td>Respond</td>
<td>Develop and implement the appropriate activities to take action in connection with a detected cybersecurity event, such as those identified in an established response plan.</td>
</tr>
<tr>
<td>Recover</td>
<td>Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.</td>
</tr>
</tbody>
</table>

And because cybersecurity risks to medical devices are continually evolving, it is not possible to entirely mitigate risks through premarket controls alone. Therefore, the FDA recommends that essential that manufacturers implement comprehensive cybersecurity risk management programs and documentation consistent with the Quality System Regulation, and to include the following critical components:25

<table>
<thead>
<tr>
<th>Monitor</th>
<th>Cybersecurity information sources for identification and detection of cybersecurity vulnerabilities and risk.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintain</td>
<td>Robust software lifecycle processes.</td>
</tr>
<tr>
<td>Understand</td>
<td>Assess and detect presence and impact of a vulnerability.</td>
</tr>
<tr>
<td>Establish</td>
<td>And communicate processes for vulnerability intake and handling.</td>
</tr>
<tr>
<td>Develop</td>
<td>Mitigations that protect, respond and recover from the cybersecurity risk</td>
</tr>
<tr>
<td>Adopt</td>
<td>A coordinated vulnerability disclosure policy and practice</td>
</tr>
<tr>
<td>Deploy</td>
<td>Mitigations that address cybersecurity risk early and prior to exploitation</td>
</tr>
</tbody>
</table>
Soody Tronson, MS/JD, has over 25 years of interdisciplinary experience in technology, business, management, education, and law in start-up and fortune 100 companies. Soody is the Founding Managing Counsel at STLG, a boutique Silicon Valley law firm counseling domestic and international clients in intellectual property and technology transactions in a wide range of technologies. Soody is also the Founder and CEO of Presque, a startup venture creating wearables that fundamentally change and improve the health of women and infants, positively disrupting the status quo. The book “Women Securing the Future with TIPPSS for IoT Trust, Identity, Privacy, Protection, Safety, Security for the Internet of Things,” which she co-authored was recently published by Springer.

After holding technical and management positions at Schering Plough and Hewlett-Packard where she took several products to market; and practicing law at HP, and a successfully acquired medical device start up, and two national law firms, HellerEhrman and Townsend and Townsend; Soody formed STLG. Presque was formed in 2017 to develop and commercialize a line of wearables based on Soody’s original design. Guided by the belief that we each have a sphere of personal influence and it is our civic duty to use it for the betterment of our community, Soody is deeply committed to creating positive change. She serves in advisory, board, and leadership capacities with several organizations including AWIS STEM to Market national Accelerator and its Palo Alto Chapter; California Lawyers Association Executive Committee of the Intellectual Property Section, Licensing Executives Society USA/Canada, and the Palo Alto Area Bar Association. As a member of the Silicon Valley Leadership Group, a diverse public policy association of dynamic companies shaping the future innovation economy, she is actively engaged with the Technology and Innovation, Health, and Education and Work Force Development, and The Women Executives Committees. One of her most fun ventures has been as co-founder of HighNote Co., a third wave coffee roasting company.


[https://www.justice.gov/criminal-ccips/cybersecurity-unit](https://www.justice.gov/criminal-ccips/cybersecurity-unit)

[https://www.oag.ca.gov/privacy/databreach/reporting](https://www.oag.ca.gov/privacy/databreach/reporting)


[https://healthsectorcouncil.org/](https://healthsectorcouncil.org/)

© STLG 2020  For General Educational Purposes Only – Not Intended as Legal Advice
19 https://healthsectorcouncil.org/hsc/joint-cybersecurity-working-group-executive-committee/

20 https://healthsectorcouncil.org/the-joint-security-plan/

21 https://www.healthit.gov/


23 https://www.healthit.gov/sites/default/files/page/2020-01/2020-2025FederalHealthIT%20StrategicPlan_0.pdf


25 FDA Publication. **Postmarket Management of Cybersecurity in Medical Devices.** DECEMBER 2016. [https://www.fda.gov/media/95862/download](https://www.fda.gov/media/95862/download)

26 [https://www.linkedin.com/in/soodytronson/](https://www.linkedin.com/in/soodytronson/)

27 STLG Law Firm. [https://www.stlgip.com/](https://www.stlgip.com/)

28 Presque. [https://www.mypresque.com/](https://www.mypresque.com/)


30 [www.highnotecoffee.com](http://www.highnotecoffee.com)