Health Sector **Coordinating Council**

Joint Security Plan (JSP)

95% of health care institutions confirm being **targeted for some form of cyberattack**

$5.5+ billion

security breach costs in the health care industry every year

There is a **62%** increase in number of connected medical devices in 5 years which is expected to accelerate.

There are over **7000** device manufacturers and smaller organizations are challenged with finding security talent for their product development.

80% of device manufacturers have less than **50 employees and need guidelines and help with security.**

The **Joint Security Plan** (JSP) is...

a consensus-based total product lifecycle reference guide to developing, deploying and supporting cyber secure technology solutions in the health care environment. It includes:

- Vendor Product Security Framework, Organization, and Program Recommendations
- Secure Product Development Best Practices
- Product Security Program Maturity Model

Why is the JSP needed?

Product cybersecurity in healthcare is a shared responsibility and has the potential to impact patient safety and clinical operations. The JSP provides recommendations that help organizations of various sizes and stages of maturity to enhance their product cybersecurity posture.

Who was involved in its **drafting**?

Public and private sector stakeholders including medical device manufacturers, healthcare IT vendors, healthcare providers, and federal agencies under the umbrella of the Healthcare and Public Health Sector Coordinating Council (HSCC)

What are JSP 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 lifecycle of medical technology

- **Maturity Evaluation:** Measuring and tracking progress of a cybersecurity program for medical technology