Quick Start Guide to Sensor Data Integration: **Data Security**

Ensure compliance local laws and regulations, recognizing that there is no one single standard, nor single agency or regulation governing data privacy in healthcare

- Review cybersecurity regulators and regulations in the U.S. and Europe in *Playbook: Digital Clinical Measures*
- Access standards pertaining to security and sensor generated data [here](https://www.dimesociety.org/tours-of-duty/sensor-data-integrations/implementation)

Expect security best practices to be built into each tier of a data architectures – the web tier, application tier, and data tier.

- Review DiMe Sensor Data Integrations cybersecurity reference data architecture

**Apply security best practices at each step of the sensor data flow**

- Apply security best practices at each step of the sensor data flow from *Playbook: Digital Clinical Measures*

**Manage security and privacy through reusable processes**

- Access resources and checklist in the [US Digital Services Playbook](https://www.dimesociety.org/tours-of-duty/sensor-data-integrations/implementation)

**Use a software bill of materials (SBOM) to reduce the security risk of including third-party connected sensor technologies in the healthcare data ecosystem**

- Learn how SBOMs provide transparency into a medical technology’s components, which can eventually reduce the feasibility of attacks [here](https://www.dimesociety.org/tours-of-duty/sensor-data-integrations/implementation)
Deploy no-cost tools from the US Federal Cybersecurity and Infrastructure Security Agency (CISA) to support your security approaches

→ Access CISA’s ransomware guide, healthcare resources, bad practices, tabletop exercise package, cybersecurity evaluation tool, and cyber hygiene services.

→ Sign up for CISA alerts and bulletins.

See quick-start guides on other ART criteria