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

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

- Review the very limited U.S. legal protections for data rights in *The Playbook: Digital Clinical Measures*
- Learn more about the EU’s General Data Protection Regulation (GDPR), the legal framework that provides the core of Europe’s digital privacy legislation
- Access standards pertaining to security and sensor generated data [here](#)

Implement privacy by design to protect patients and build trust in connected sensor technologies and healthcare data ecosystem ecosystems

- Review privacy by design principles in *The Playbook: Digital Clinical Measures*

Ensure that the end-user license agreements (EULAs) and terms of service (ToS) of connected sensor technologies and data platforms are congruent with local laws, regulations, and informed consent

- Learn more about EULAs and ToS in *The Playbook: Digital Clinical Measures* and DiMe’s *Primer on Digital Medicine: Measurement*

Manage security and privacy through reusable processes

- Access resources and checklist in the [US Digital Services Playbook](#)
Conduct a data protection impact assessment when sensor data is likely to involve “a high risk” to other people’s personal information

→ Access the EU’s GDPR [data protection impact assessment template](#)