Update and Overview of GMTA Principles and Position Papers

Zach Rothstein
GMTA

IMDRF Open Stakeholder Day
Wednesday, March 21, 2018
Shanghai, China
Who Are We?

- Origins date to 1990s as informal network

- Formally established in 2010 with Secretariat and website in Geneva; legally constituted in Switzerland as an “association” in 2013; WHO recognized NGO in 2015

- Membership open to medical technology associations (not companies):
  - Willing to accept GMTA governance rules
  - With functioning code of ethical business practices
With 25 member associations, here are the countries represented by GMTA...
GMTA Principles and Position Papers

• UDI
• Cybersecurity
• Registries
• Real World Evidence

Available at GMTA’s website: globalmedicaltechnologyalliance.org
GMTA UDI White Paper
UDI Principles

1. Rules should be phased-in and based on risk
   - Initial implementation timeline should be two years or more

2. Rely on standards and globally accredited issuing agencies
   - Manufacturers already work with existing globally accredited issuing agencies (e.g. GS1, HIBCC, ICCBBA, GMDN)
UDI Principles

3. Regulators should provide on-going assistance to industry
   – Help desk, training, and public communications

4. Include a mechanism to request exception, exemptions, alternatives, and extensions of time
   – Enables manufactures to address implementation challenges in a positive and constructive manner
UDI Principles

5. Date of manufacture should not be a required element of the production identifier unless no other production identifier is available

- Including DOM in PI presents many technical challenges

6. UDI rules should not apply to devices manufactured or labeled prior to the rule’s compliance dates

- Locating, removing, storing, and/or reworking devices after the compliance date to either re-label or destroy is unproductive and could lead to product shortage
UDI Principles

7. Triggers for a new device identifier should be limited to the rules of the UDI issuing entities

- Not all product changes should require a new DI
- Reflected in CFDA’s UDI Rule
GMTA Cybersecurity Principles
Cybersecurity Principles

• Objective
  – Provide principles for use by the medical technology industry to establish effective cybersecurity for its medical devices
  – Demonstrate the device industry’s commitment to patients and health care practitioners to provide secure medical device

• Application
  – Applies to connected devices only (for example, devices that connect via internet, hospital networks, or directly to another medical device)
Cybersecurity Principles

1. Medical device development and security risk management
   - Cybersecurity risk management program that incorporates both premarket and postmarket phases

2. System level security
   - Shared responsibility for security incidents to be investigated collaboratively
Cybersecurity Principles

3. Coordinated disclosure

   – Establishment of coordinated disclosure process for researchers to submit findings

4. Consensus standards, regulatory requirements, and education

   – Cooperative effort among regulators, manufacturers and security experts to develop standards and regulations
GMTA Registry Principles
Registry Principles

• Objectives for a registry
• Threshold questions
• Data governance
• Policies for use and publication of data
Registry Principles

• Objectives for a registry

  – Improve patient care and outcomes
  – Improve patient access to new therapies
  – Evaluate safety and/or effectiveness of product
  – Meet regulatory requirements for postmarket surveillance
Registry Principles

• Threshold questions
  – Do objectives warrant the level of investment required to develop and maintain a registry?
  – Is registry the least-burdensome means to collect the necessary data to achieve the scientific objectives?
  – Are there reliable data collection instruments available to collect the data?
  – Will the registry have a stable and diverse source of funding to promote long-term sustainability?
Registry Principles

• Data Governance
  – Rules governing access to data
  – Process for data request review
  – Controlled process for data release
  – Process for device safety data reporting
Registry Principles

• Policies for use and publication
  – Company access to own data and aggregate data
  – Safety signals reported to company for further investigation
  – Regulatory bodies seek input from company before taking regulatory action based on registry data
  – Protect against unauthorized use of data and ensure appropriate transparency
GMTA Real World Evidence Principles
Real World Evidence Principles

• Real world evidence includes data collected from a variety of sources, such as:
  
  – Registries
  
  – Public and private health plans
  
  – Manufacturers
  
  – Electronic health records (EHR)
  
  – Regulators
Real World Evidence Principles

• Potential benefits of real world evidence include:
  – Improve patient care and outcomes
  – Improve patient access by expanded use and indications
  – Support streamlined device modifications
  – Enhance postmarket data collection
Real World Evidence Principles

1. System has clear purpose, objective, and participation requirements
   - Data must be of appropriate quality for intended use; data integrity and security must be maintained

2. System overseen by data governance committee
   - Inclusive of manufacturers, the committee should set criteria for data ownership, access, and use
Real World Evidence Principles

3. Regulators have clear policies for use of RWE
   - Information shared with manufacturers prior to taking action

4. Data access
   - Qualified scientific, medical and economic researchers to benefit health or patient care
   - Manufacturers’ permitted full and timely access to data on their products
Real World Evidence Principles

5. Compliance with applicable laws and regulatory requirements

– Protection of patient privacy; informed consent obtained

– Protection of all confidential, proprietary information from release