Consideration of Cybersecurity vs Safety Risk Management

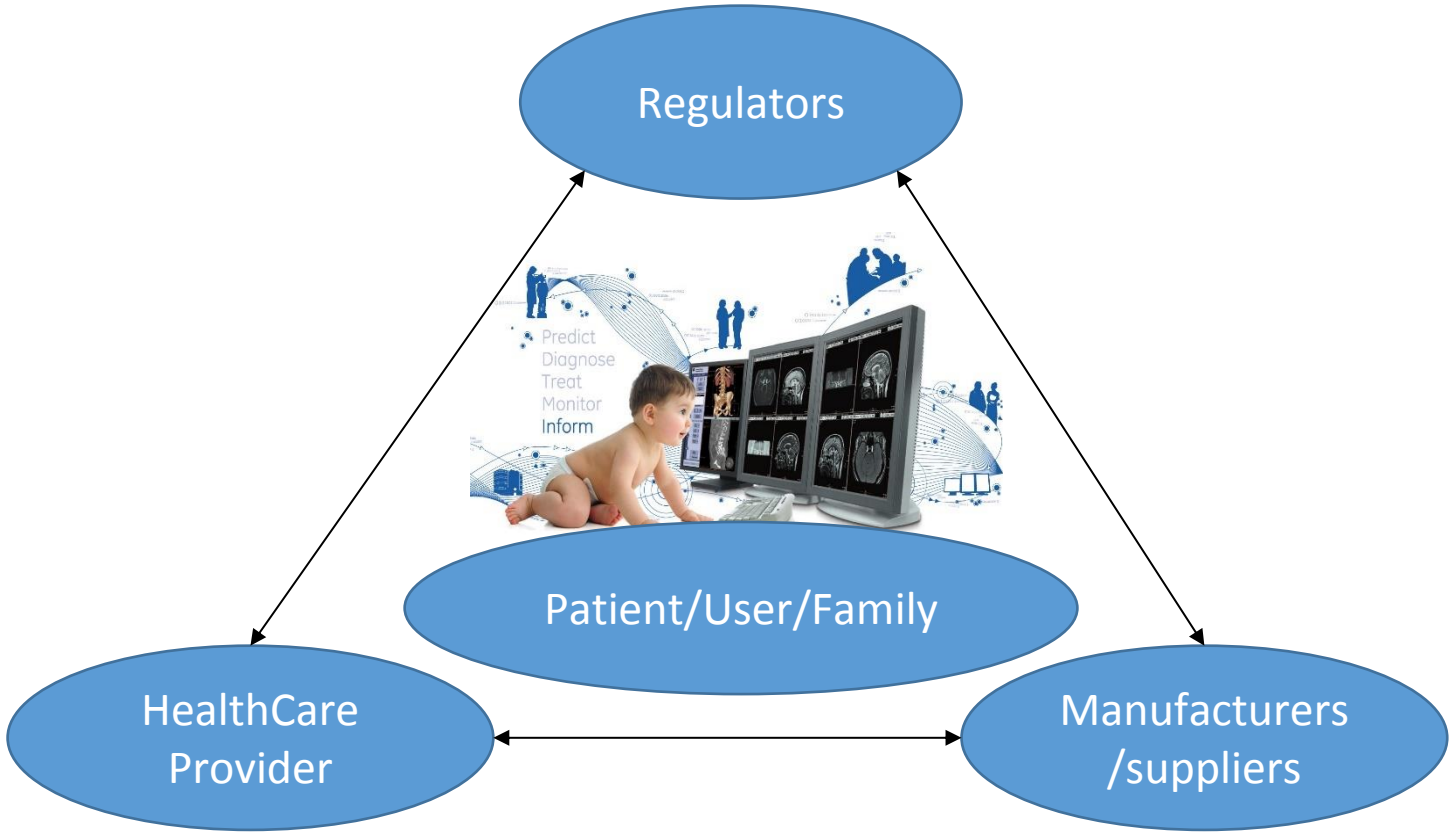
Weiping Zhong, Ph.D.
Global Director of Risk Management/Medical Devices
GE Healthcare

DISCLAIMER: The views and opinions expressed in this presentation are for academic discussions and are those of the authors and do not necessarily represent official policy or position of GEHC.

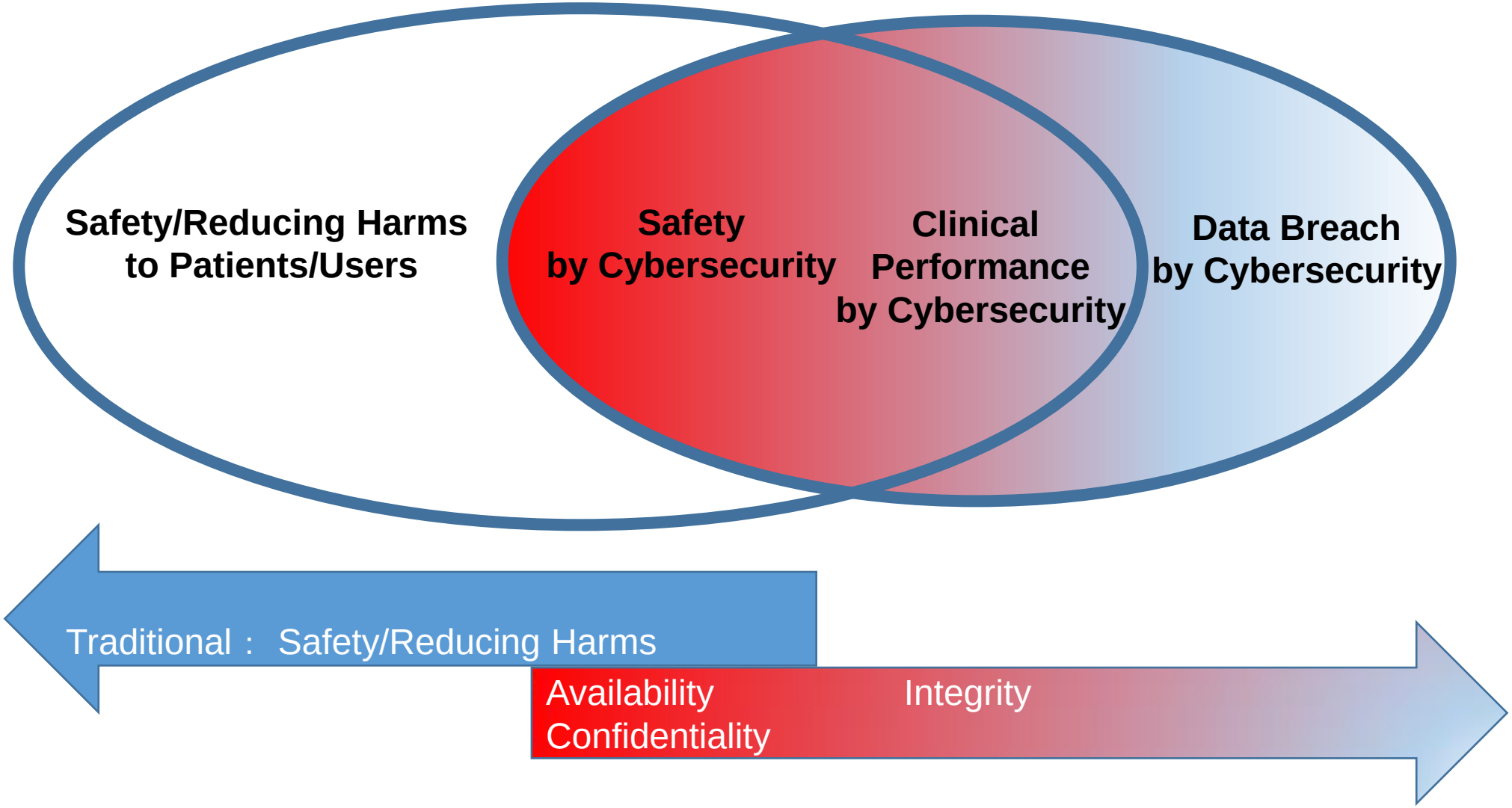
Agenda:

- Background and Purposes: Who & What?
- Regulatory Dynamics on Cybersecurity: How?
- Concepts: ISO14971 & Cybersecurity (AAMI TIR 57）
- Challenges and Forward Thinking: …
- Summary

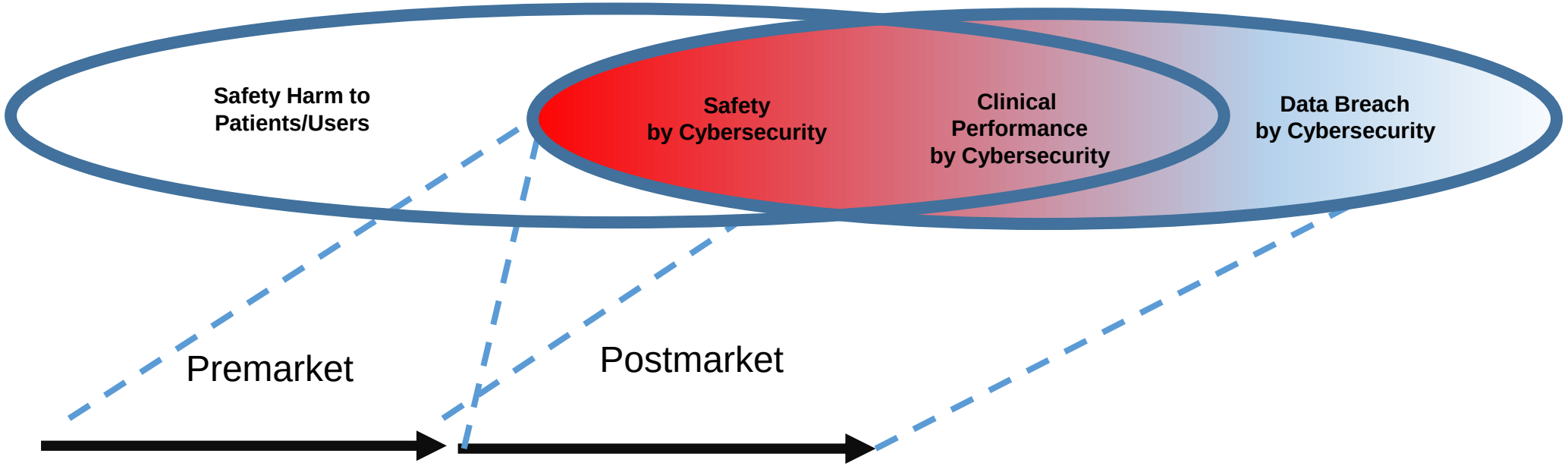
Who and What?


Regulators
Predict
Diagnose
Treat
Monitor
Inform
Patient/User/Family
HealthCare Provider
Manufacturers /suppliers

Cybersecurity & Safety Risk Management

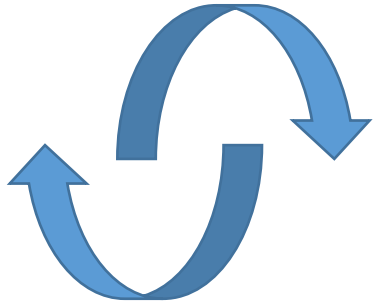


Applying similar concepts



- Identify Risks
- Propose Requirements
- Implement Mitigations
- Verify and Validate
- Document & Submit

- Monitor Feedback/Complaints
- Report Injuries
- Determine Field Actions
- Determine Recalls



Examples of Regulations

FDA: FDA Pre & Postmarket Guidance

- Mitigate from design/development
- Documentation
  - Hazard Analysis and Design Mitigations
  - Traceability Matrix between Risks & Controls
  - A Summary of Plan: validated updates, lifecycle , patches
  - Labeling
- Process:
  - Cybersecurity Risk Management system: leveraging ISO 14971 & Quality Management System
  - Recall decision

European Union: Standards + Directive/Regulation

- Cybersecurity: design
- EN ISO 14971, EN 45502 and EN 62304
- Data Protection Directive/General Data Protection Directive
- Data Protection: “by design and by default”
- Risk Assessment and Mitigations are required

CFDA Submission Guidance

- Life-cycle Risk-based approach: safety focused
- Establish traceability on validation
- Documentations (3 types)
  - Major changes affecting Safety/Effectiveness
  - Minor changes not affecting Safety
  - No changes

How?

Patients/Customers

Regulators

Manufacturers

Patients'/Customer's need

Regulation

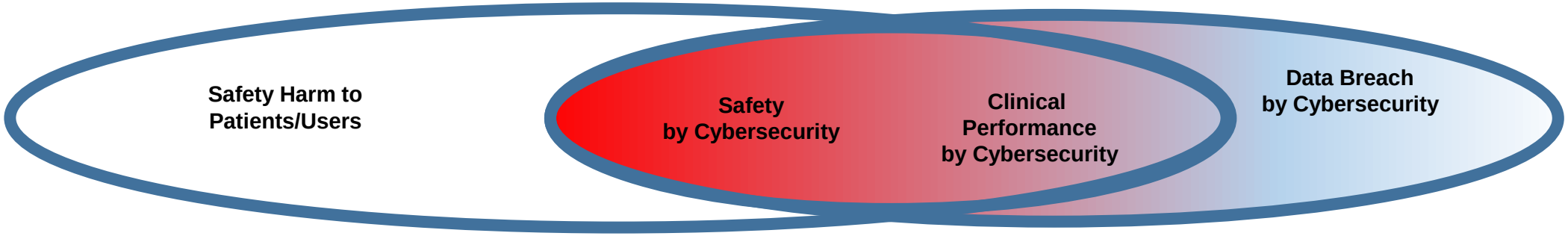
Quality/Risk Management

more

Engineering:
R&D, Production

Post-production
& Service

A Concept:
ISO 14971 vs Cybersecurity



ISO 14971

- Top Management Responsibility
- Risk Management Plan
- Risk Analysis/Evaluation/Control
- Acceptability: Residual Risk
- Risk Management Report
- Production/Postproduction

ISO 14971: Medical Device
Risk Management

AAMI TIR 57

- Top Management Responsibility
- **Security** Risk Management Plan
- **Security** Risk Analysis/Evaluation/Control
- Acceptability: **Security** Residual Risk
- **Security** Risk Management Report
- Production/Postproduction

AAMI TIR 57
Principles for medical device
security—Risk management

A Concept: ISO 14971 vs Cybersecurity

FDA:
Post-market
Guidance

ISO 14971:
Risk Matrix

	Negligible	Minor	Serious	Critical	Catastrophic
Frequent					
Probable	R_1	R_2			
Occasional		R_4		R_5	R_6
Remote					
Improbable			R_3		

FDA's Postmarket Guidance

- **Severity of Harm = ISO 14971**
  - Catastrophic: Death
  - Critical: Permanent impairment/life-threatening
  - Serious: Injury/imp. requiring professional medical intervention
  - Minor: temporary injury/impairment
  - Negligible: inconvenience or temporary discomfort
- **Exploitability**
  - High
  - Medium
  - Low

A Concept: Criteria for Acceptability

- FDA's Postmarket Guidance
- **Controlled** sufficiently low (acceptable) residual risk of patient harm

- **Uncontrolled** unacceptable residual risk of patient harm due to inadequate … mitigations

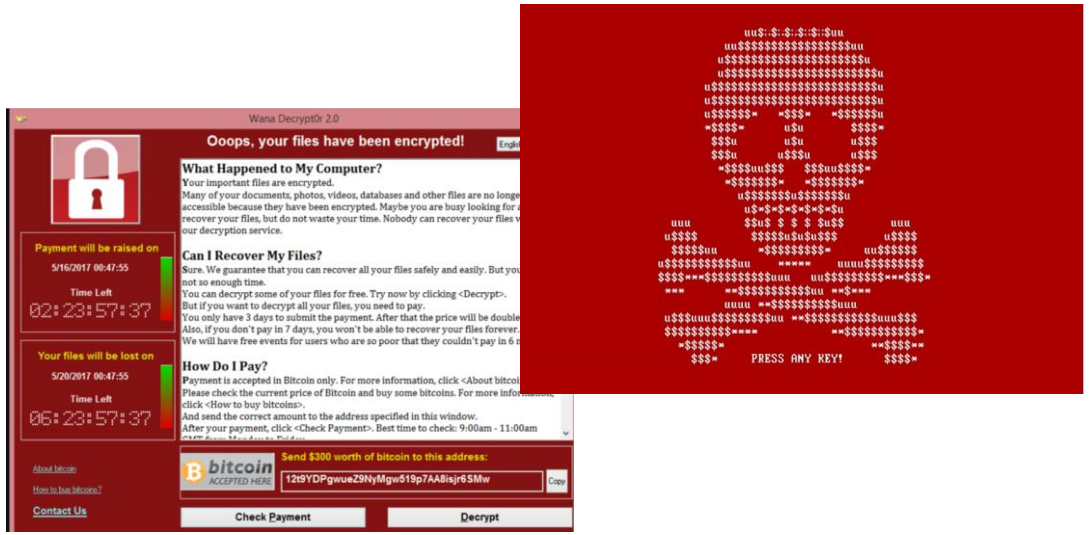
- ISO 14971:

- Overall residual risks ➔ acceptable

Password: #%$!$@%#

Challenges and Forward Thinking

- **Purpose:** Intended Use vs Malicious Intend
- **Technical:** System is “static”, Cyberattacks are “dynamic”
- **Regulatory vs Operational:**
  - “existing system” ---- New challenges
  - Traditional “lengthy” processes vs “speed”
- **Responsibility:** shared responsibilities among key stakeholder
- **Information Sharing vs Confidentiality**
- **Critical Infrastructure and National Security**
- **Large number of requirements vs Standardization**



Summary

- Background: Why and What?
- Regulatory Dynamics on Cybersecurity: How?
- Concepts: ISO14971 ←→Cybersecurity
- Challenges and Forward Thinking
- Questions