国立大学法人
九州工業大学

Medical IoT Devices and Systems: Challenges and Opportunities

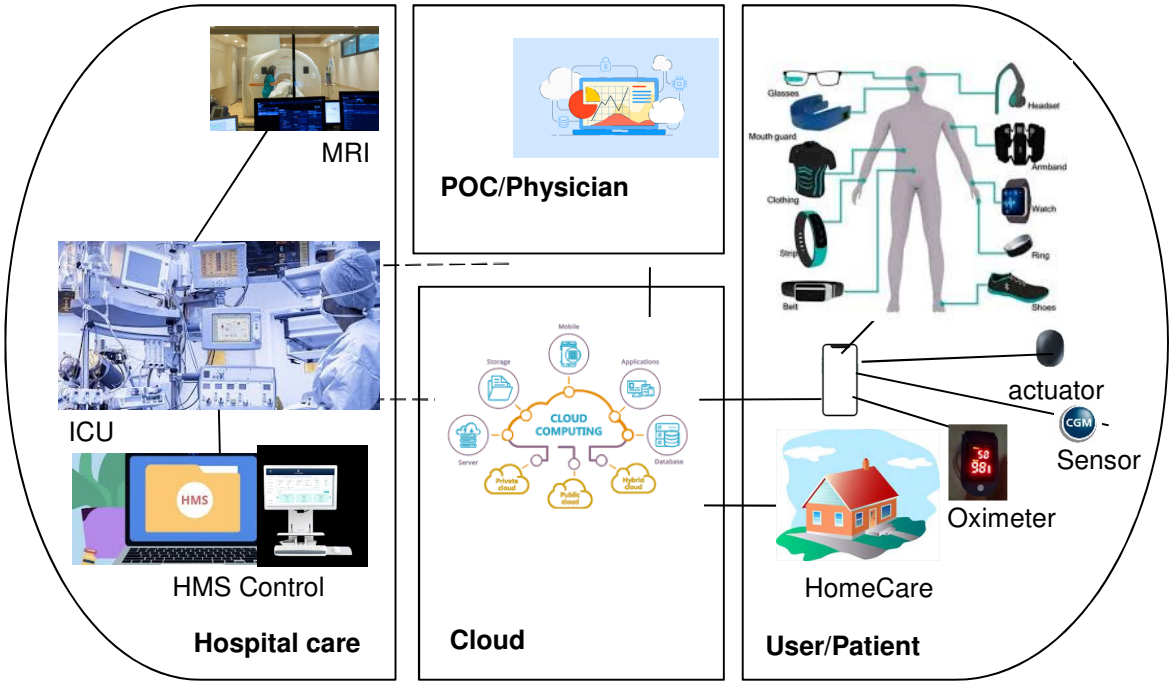
Dirceu Cavendish,

Daiki Nobayashi, Takeshi Ikenaga

Modern Medical Systems

Medical Systems Components

- Small edge device: implants (e.g. pacemakers), sensors (e.g. cgm), actuator (e.g. pump)
  - Short range communication: battery/security
- Command and control device: smartphone
- Cloud infrastructure
  - Data gathering and health care professional analysis/reports
  - System security control
- Hospital infrastructure
  - ICU/MRI/etc
  - Hospital Management System



Related service verticals

- Home management: home health care
- Transportation: Emergency services

Health Care Biomarkers

Biomarkers: measurable indicators of a biological state or condition. Indicators may include molecules, genes, proteins, etc. Biomarkers may be extracted from blood, urine, tissues, etc.

Biomarker types:

- Disease detection and diagnosis: Before symptoms appear.
- Prognosis: severity and progression of a health condition/disease
- Monitoring: treatment response/effectiveness
- Personalized treatment: tailored to specific patient
- Drug development support: support of clinical trials in innovative treatments
- Disease Risk Assessment: Identify individuals' likelihood of developing a disease

Biomarker tracking:

- Slow varying: Takes months to significant changes => lab exams tracking
- High varying: Takes days/hours to display significant changes => wearable **sensors**

Comp. Metabolic Panel (14)

	Test	Current Result and Flag		Previous Result and Date		Units	Reference Interval
▲	**Glucose** [03]	**107**	**High**	95	02/25/2025	mg/dL	70-99
	BUN [03]	15		19	02/25/2025	mg/dL	8-27
▼	**Creatinine** [03]	**0.72**	**Low**	**0.73**	02/25/2025	mg/dL	0.76-1.27
	eGFR	105		104	02/25/2025	mL/min/1.73	>59
	BUN/Creatinine Ratio	21		**26**	02/25/2025		10-24
	Sodium [03]	138		138	02/25/2025	mmol/L	134-144
	Potassium [03]	4.1		4.3	02/25/2025	mmol/L	3.5-5.2
	Chloride [03]	103		102	02/25/2025	mmol/L	96-106
	Carbon Dioxide, Total [03]	21		25	02/25/2025	mmol/L	20-29
	Calcium [03]	9.1		9.0	02/25/2025	mg/dL	8.6-10.2
	Protein, Total [03]	6.9		7.0	02/25/2025	g/dL	6.0-8.5
	Albumin [03]	4.3		4.2	02/25/2025	g/dL	3.8-4.9
	Globulin, Total	2.6		2.8	02/25/2025	g/dL	1.5-4.5
	Bilirubin, Total [03]	0.8		0.9	02/25/2025	mg/dL	0.0-1.2
	Alkaline Phosphatase [03]	84		76	02/25/2025	IU/L	44-121
▲	**AST (SGOT)** [03]	**55**	**High**	**66**	04/29/2025	IU/L	0-40

Biosensors

Oximeter
- Measures: Lungs Oxygen Saturation Level; heart rate
- Abnormalities: Pneumonia; Blood Clots; Covid-19.

Glucose Monitors
- Measures: Glucose levels in interstitial fluid (skin)
- Abnormalities: Diabetes; Obesity; Insulinomia

Cholesterol Monitors (smart contact lenses*)
- Measures: Cholesterol levels in tear fluid
- Abnormalities: Hyperlipidemia; Cardiovascular diseases

Electronic tattoos (graphene)
- Measures: heart rate; blood pressure;
- Abnormalities: Cardiovascular diseases

Activity Auxiliary Data (smatwatch/fitbit)
- Measures: steps data; activity classifiers (data context); sleep data;
- Biosensor data correlation: Heart rate; Glucose levels;

Prof. Man Bock Gu, Korea University, Biosensors and Bioelectronics, April2024: “In biology and medicine, however, time is an overlooked and mostly forgotten variable. This is the reason why most healthcare systems rely on single set of measurements at a clinic to evaluate the health of an individual and diagnose diseases. **With the emergence of the new paradigm of continuous sensing, we are now moving toward capturing biological processes and responses without losing the important, time-dependent changes.** Especially in the dawn of the revolution of artificial intelligence, large datasets of high quality, continuous-time data can help us detect anomalies rapidly in an individualized fashion. These new datasets would also enable us to discover new biological pathways, processes and chemicals.”

* Wireless Non-Invasive Monitoring of Cholesterol Using a Smart Contact Lens, H. Song et. al., https://onlinelibrary.wiley.com/doi/10.1002/advs.202203597

Medical Device Security Landscape

Medical components vulnerabilities/threats

- Edge devices;
  - implants: lack of encryption/authentication – injection of malicious commands
  - sensors: lack of FW authentication, lack of encryption/integrity check – data tampering/MITM attacks
  - Lack of (secure) FW over the air updates
- Smartphones
  - OS vulnerabilities: (CVSS); Generic notification mgm – lack of medical device app category.
  - Common Apps vulnerabilities: lack of authentication/attestation verification; lack of App protection framework (e.g., DexGuard, zShield); unauthorized data harvesting;
- Cloud infrastructure/resources
  - Resources' outages - DoS
  - Dependency on PKIs/certificates
- Hospital infrastructure
  - Legacy equipment: Obsolete OS, hardcoded credentials, lack of database encryption – code injection, ransomware
  - Hospital Management System: Requires strong Identity and Access Management (IAM); Requires PHI role based access control

Medical Systems Security Requirements

Embedded/SW Secure requirements

- Firmware tampering verification
- Firmware/software compatibility (Versioning)
- Configuration/calibration verification
- OS security patching

Components Authentication and Authorization

- Short range authentication: secure BLE (IoT whitelisting)
- System Multifactor authentication
- Explicit resource authorizations via security tokens
- Cloud Hardware Security Module (HSM): management of security credentials

Medical Systems Safety Regulations

International Regulations

- ISO 13485 Quality management systems
  - Design Controls, verification and validation
- ISO 14971 Risk Management of medical devices
  - Risk Identification and quantization;
  - Risk controls, residuals, and mitigations;

Medical Systems Privacy challenges

Unreadable/unenforceable EULAs
- Cumbersome End-User License Agreements
- Click through services

Controlled data sharing
- Health personal data sharing with medical personnel only
- Massive data gathering (unprocessed medical data)

Third party medical data gathering
- Primary care physician/nurse computer systems
- Point of care security (hospital outdated systems)
- Cloud partners: Medical data gathering companies

.

Technology failures
- Embedded device hacking: limited HW capabilities, small SW footprint
- Cloud system miss-management
- Cryptographic material leaks

Medical Systems Security/Privacy Regulations

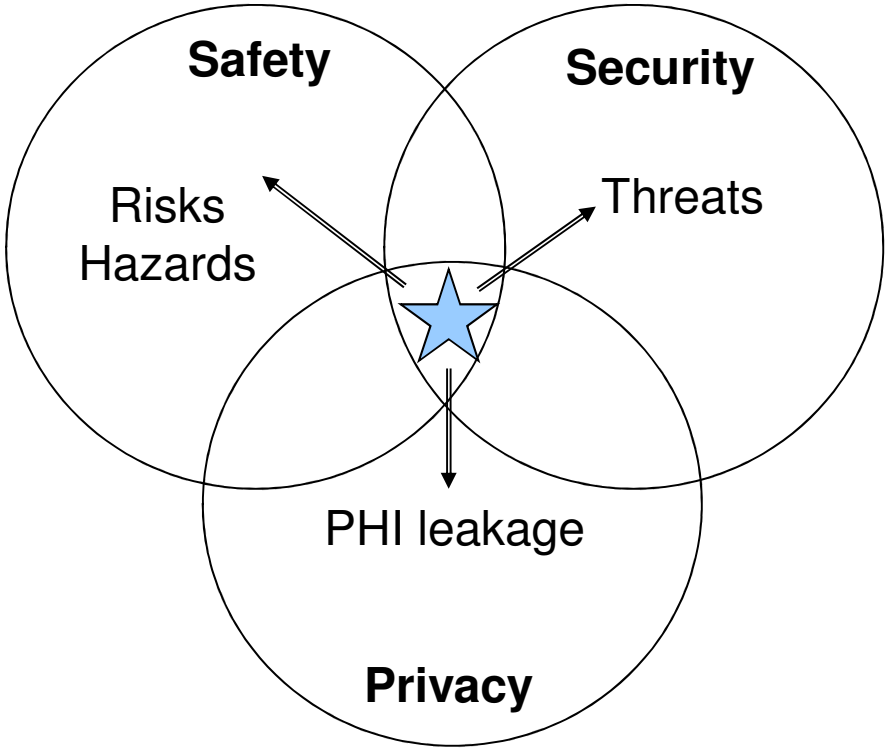
Strong regulatory mandates

- FDA Code of Federal Regulations: Part 11 Medical devices
  - SSL encryption (at rest, in transit);
  - Restricted access;
  - Access control;
  - Data audit trail;
  - Version control;
  - Digital signature
- GDPR: General Data Protection Regulation
  - Minimal data collection (purpose)
  - Right to data report
  - Right to data correction
  - Right to be forgotten
  - Right to opt-out data storage/processing/sharing
  - Data portability

Security, Safety, and Privacy

Tradeoff Scenarios

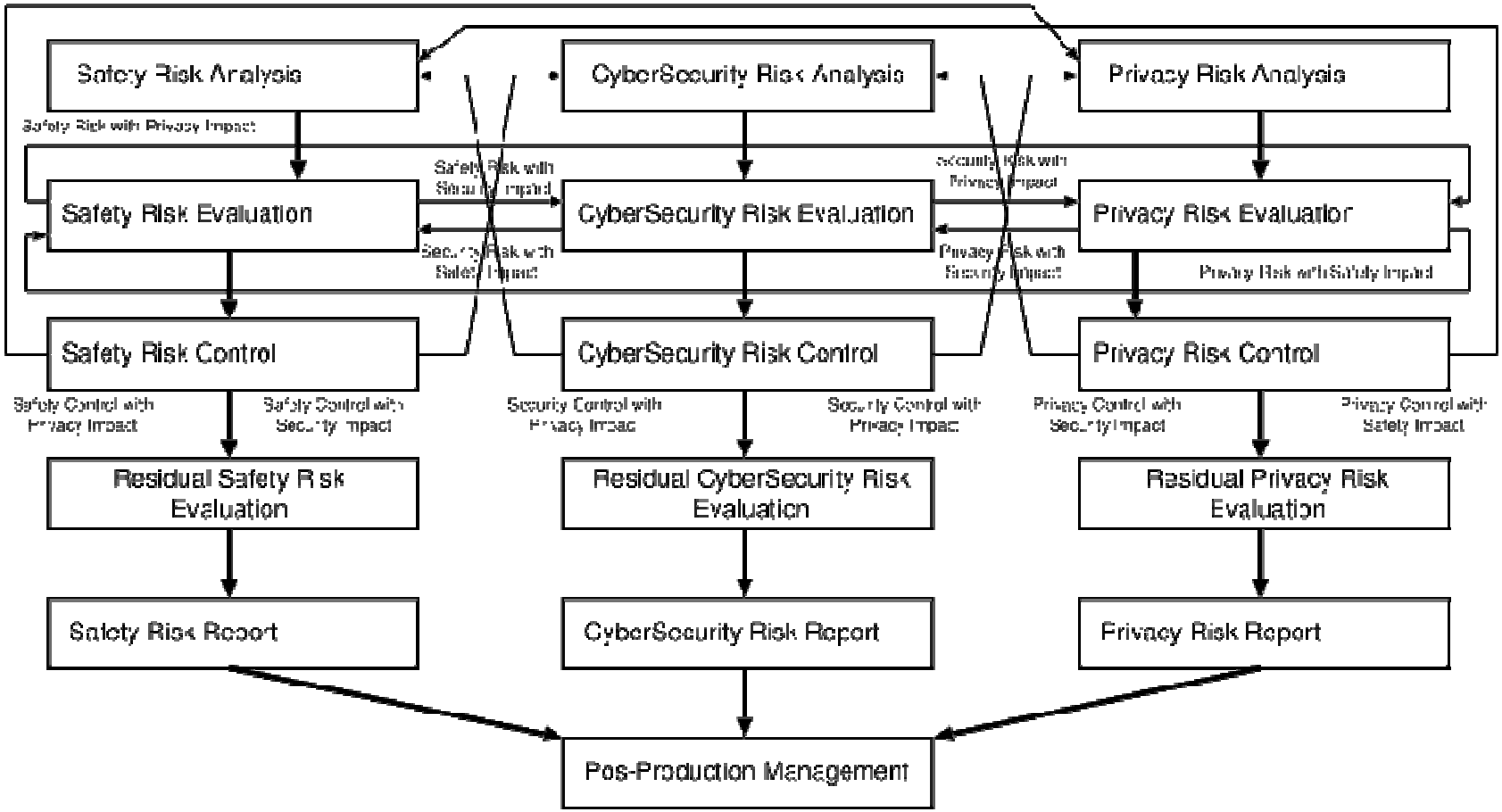
- Safety/Privacy: Deny PHI access to healthcare professionals
- Safety/Security: Stop Therapy on security threat detection
- Security/Privacy: Block patient data access on security threat



Security, Safety, and Privacy Risk Analysis

ISO 14971 Risk Analysis extension

- Consider Cyber and Privacy Risks
- Risk impact across risk types
- Risk Control impact across risk types



* ISO 14971: 2019 Medical devices – Application of Risk Management to medical devices

Health Care Delivery Evolution

Current Health Care

- Once/twice primary care physician checks
  - 6 mo/1year snapshot of vitals/performance indicators (screening tests): lipids, etc.
  - Referral to specialist if something is out of ordinary
  - Prescriptions as per needed – side effects self monitoring

Data Driven Health Care

- Real time monitoring of vitals/performance indicators by physician.
- Automatic data scanning for abnormalities.
- Physician visit scheduling triggered by abnormalities
- Specialist contacting with further data analysis.
- Specialist visits by specialist invitation
- Prescriptions as per needed – side effects evaluation via data collection

Medical Data Ecosystem

Descriptive Data

- Patient Health Information: age, gender, ethnicity
- Biomarkers' data
- Environment data: location, work activities; sports activities
- Data outcomes: Admission statistics; Mortality Rates; Infection Rates;

Assisted Diagnostics

- Verified illnesses may have specific data lakes, to support research/diagnosis
- Patient anonymized data will feed data lakes.
- AI/Machine Learning techniques (e.g., LLM) may improve diagnosis time and accuracy
- Data outcomes: From patient symptoms/data, likelihood of a given illness;

Predictive/prescriptive Analytics

- Patient outcomes: Mortality rate; medication reactions
- Customized (race/genetics) Treatments: options and risks; medications and side effects

Challenges of AI/ML techniques in Medical Systems

Applied AI/ML techniques in Medical Systems

- Diagnosis
- Therapy delivery
- Outcome Prediction

AI/ML Diagnosis:

- Quality/relevance of training datasets: different diseases require distinct data
- Verification of results: subject matter expert (MD)
- Data privacy – anonymization of training data
- Cybersecurity – Learning model attacks

AI/ML therapy delivery:

- Safety of AI/ML based therapy delivery: guardrails
- Effectiveness of AI/ML therapy delivery
- Cyber attack detection and mitigations

AI/ML based treatment outcomes prediction

- Prediction monitoring vis a vis real outcomes
- Precision metrics: cure, health improvement, health deterioration
- Explainability of predicted vs real outcomes and model corrections

AI/ML Medical Workflows

Safe and effective workflows
- AI/ML as an assistant to MD
- MD expert verification of outcomes
- Automatic guardrails

Diagnosis:
- Patient interview/consultation may be aided by medical LLM (specific medical databases)
- Diagnosis Hypothesis testing: Investigative patient data, aka Lab testing and patient specific medical diagnostic procedures (imaging – Xrays, MRI) may be aided by AL/ML techniques – disease vs data signature correlation.

AI/ML therapy delivery:
- Therapy effectiveness/safety: patient data monitoring during therapy.
- Establishment of data driven guardrails to re-evaluate therapy (e.g., biomarkers safe range boundary detection)
- Side-effects control and therapy adjustments.

AI/ML treatment outcomes
- Feeding patient illness journey back to medical databases. Case by case Learning.
- Workflow adjustments for better outcomes

国立大学法人
九州工業大学

Thank You

Questions?

Dirceu Cavendish