Panel IV: Challenges: The Digital Health Platform (System of Systems)

Moderator: Julian M. Goldman, MD, Harvard Medical School, MGH, Partners HealthCare

Regulatory Ambiguity and Requirements for ‘New Devices’
Bakul Patel, FDA

Medical Device Supply Chain Challenges
Ken Herold, Windriver

Security Design Implications: Safety and Privacy
Steven Abrahamson, GE Healthcare
Aligning National Science & Technology Resources to deliver a platform for healthcare innovation to improve patient safety

Julian M. Goldman, MD
Director, Program on Interoperability, Mass General Hospital Medical Director, Partners HealthCare Biomedical Engineering Anesthesiologist, MGH/Harvard Medical School

Contact information: www.jgoldman.info
How Many Die From Medical Mistakes in U.S. Hospitals?

A New, Evidence-based Estimate of Patient Harms Associated with Hospital Care

John T. James, PhD

• 1999 IOM published “To Err Is Human” up to 98,000 people a year die because of mistakes in hospitals.
• 2010 the Office of Inspector General for Health and Human Services said that bad hospital care contributed to the deaths of 180,000 patients in Medicare alone in a given year.
• 2013 Journal of Patient Safety: between 210,000 and 440,000 patients each year who go to the hospital for care suffer some type of preventable harm that contributes to their death.
• “That would make medical errors the third-leading cause of death in America, behind heart disease, which is the first, and cancer, which is second. “

Who is responsible for fixing these problems? Who is empowered? What is the solution pathway?
Proposal: Can digital health platforms add “error resistance” to healthcare delivery?
Devices, processes, non-integrated system → errors
Clinicians need timely, accurate data. Business process automation could help reduce error, treatment delays, injuries and deaths. *Is that how we practice today? Where are innovative solutions?*
Pulse Oximeters measure oxygen saturation – displayed as $\text{SpO}_2 \%$

Pulse Oximeter and EMR show oxygen saturation of 84% and pulse rate.
Medical Devices:
Also the “Last Mile”
data back to devices

Example - Infusion technology:
1. Decision support?
2. Prevent contra-indicated infusion?
3. “Artificial pancreas” Capabilities? (closed loop)
4. Consolidate all data for adverse event analysis?
5. Check device status, software version? Recall?

Infusion pumps for use on ONE patient
Patient Controlled Analgesia (PCA)

1. 6.5% of 2009 events in FDA MAUDE voluntary reporting database over two-year period = 65 harmed patients/year.
2. Actual number of events: Up to 6,875 serious preventable PCA-related adverse events occur annually.
3. Based on $13,803 per injured patient, economic impact is approximately $15-145M annually.
BP cuff - Pulse Oximeter Interaction

- Not real event
- “Bad” data

Baseline

Cuff inflates – loss of finger signal

Blood returns to finger
A MAN with one clock knows what time it is, goes the old saw, a man with two is never sure. Imagine the confusion, then, experienced by a doctor with dozens. Julian Goldman is an anaesthetist at Massachusetts General Hospital in Boston. Like many modern health care facilities, it has become increasingly digitised and networked, with hundreds of high-tech medical devices feeding data to a centralised electronic medical record (EMR), which acts as both a permanent repository for health information and a system that can be accessed instantly by doctors to assist with clinical decisions.
Monitor Displays Low Oxygen Level (SpO₂) Alarm Event “84%” at 2:07

All clinical data is not necessarily transmitted to EHR

No evidence of 84% SpO₂ in EHR (Blue ticks representing SpO₂ values Don’t change)
The Internet of Things

Connect the World

IV Start Pak
Apps store for smart alarms; med safety

What if...

“Internet of Things for Health Care”

Asking a lot of the platform
OpenICE Open-Source Digital Research Platform (MGH)

Based on ASTM F2761 “Essential safety requirements for equipment comprising the patient-centric integrated clinical environment (ICE)

www.openice.info

Testbed funded in large part by NIH, NSF, and DoD
“Prototype Healthcare Intranet to Improve Health Outcomes”
Safety Culture

INFORMED CULTURE
Those who manage and operate the system have current knowledge about the human, technical, organisational and environmental factors that determine the safety of the system as a whole.

REPORTING CULTURE
An organizational climate in which people are prepared to report their errors and near-misses.

JUST CULTURE
An atmosphere of trust in which people are encouraged (even rewarded) for providing essential safety-related information, but in which they are also clear about where the line must be drawn between acceptable and unacceptable behaviour.

FLEXIBLE CULTURE
A culture in which an organisation is able to reconfigure themselves in the face of high tempo operations or certain kinds of danger - often shifting from the conventional hierarchical mode to a flatter mode.

LEARNING CULTURE
An organisation must possess the willingness and the competence to draw the right conclusions from its safety information system and the will to implement major reforms.

Based on Reason, Managing the Risks of Organisational Accidents, 1977

http://www.coloradofirecamp.com/just-culture/definitions-principles.htm
Recommendation #1

Develop open, interoperable, medical device – HIT ecosystem platforms to unleash innovation of sensors, actuators, and analytics while enabling crowd-sourcing of solutions to current and future capability needs/hazards

- Shared testbeds with standards reference implementations
- Data Logging
- App development
- Suitable for “safety critical” applications
- Rich, contextual data for BIG DATA analytics
 Recommendation #2

Alignment of national science & technology resources to develop, deploy, iterate IoT* for Health Care (build on CPS initiative)

- Use rich, contextual data to measure, baseline, create solutions
  - Planes, trains, automobiles have data loggers – essential for safety critical environments
- Require data for CMS reimbursement – pay for never events (only if data is provided)

* = Internet of Things
Can our nation deliver these capabilities? there are many S&T Gaps ...

- Security of networked medical devices
  - Cost
  - Balance security and usability
- Composability - Healthcare delivery organizations and other system integrators must be able to compose reliable systems of devices from diverse manufactures (hardware and apps)
- Standards gaps/lack of reference implementations
- Interoperability chasm
- Software reliability and life-cycle management
- Etc.

See white paper: http://mdpnp.org/HITSA.html
If this was a medical moonshot, Who would benefit? Who would contribute?

AMC; Universities

Medical Device Industry
Is NITRD the right “home” OSTP?
Plug-and-Play Network Devices

Another enabling technology for the aforementioned vision is the development of plug-and-play networking technology for medical devices. Plug-and-play capability is needed to ease the setup of integrated point-of-care and extramural arrays of medical devices that communicate with a patient’s electronic health record.

Devising the technology would require addressing concerns about privacy, security, safety, regulations, and technology. In hospital settings, for example, networks would form and reform frequently, as patients are admitted and discharged. Technology for the rapid formation of ad hoc networks needs developing. At the same time, authentication mechanisms would be needed to
“The December 2010 report of the President's Council of Advisors on Science and Technology (PCAST) titled Designing a Digital Future: Federally Funded Research and Development in Networking and Information Technology calls for continued investment in CPS research because of its scientific and technological importance as well as its potential impact on grand challenges in a number of sectors critical to U.S. security and competitiveness such as the ones noted above. These challenges and technology gaps are further described in a CPS Vision Statement published in 2012 by the Federal Networking and Information Technology Research and Development (NITRD) Program's CPS Senior Steering Group.”

Wikipedia: The US National Science Foundation (NSF) has identified cyber-physical systems as a key area of research. Starting in late 2006, the NSF and other United States federal agencies sponsored several workshops on cyber-physical systems...
Yesterday, the National Science Foundation (NSF) announced a new partnership with the U.S. Department of Homeland Security Science and Technology Directorate (DHS S&T) and U.S. Department of Transportation (DOT) Federal Highway Administration (FHWA), issuing a first-ever interagency solicitation for Cyber-Physical Systems (CPS). Leveraging years of investment in CPS science, engineering, and technology by NSF's Directorates for Computer and Information Science and Engineering (CISE) and Engineering (ENG), the new solicitation establishes collaborations between NSF and mission agencies to “identify basic research needs in CPS common across multiple application domains.”
It all began with a new way of thinking.
MD PnP Program of Work Supported in Part By:

- Department of Defense US Army Medical Research and Materiel Command, award numbers W81XWH-12-C-0154 and W81XWH-09-1-0705
- NIH/NIBIB, grant number 1U01EB012470
- Department of Defense US Army Medical Research Acquisition Activity, award number W81XWH-09-2-0001
- National Science Foundation, grant numbers CNS-10-35715, IIS-1239242, CNS-08-34524, and CNS-08-34709
- National Institute of Standards and Technology, grant number 70NANB10H258

The contents of this presentation are solely the responsibility of the MD PnP Program and do not necessarily represent the official views, opinions, or endorsements of the granting agencies.