Directions in Connected Medical Device Norms

Michael Aisenberg, Esq.
Senior Fellow, GWU Center for Cyber & Homeland Security

NAAG Southern Region Spring Conference
Implantable medical devices can be hacked to harm patients.

*The way to a man's heart is through his pacemaker's security flaws, researchers say.*
WIRED:
Medical Devices Are the Next Security Nightmare
THE SERIOUS AND IMENSE IMPACT OF A MEDICAL DEVICE HACK

• 21 FOOTNOTES !!!
BBC NEWS:
Medical devices vulnerable to hackers
USA TODAY:
– Medical-device, IoT hacks spurring security software boom

POPULAR SCIENCE HEALTH
– Hacked Medical Devices May Be The Biggest Cyber Security Threat In 2016
  • Through insulin pumps and pacemakers, hackers could hold your life ransom

abc NEWS
– FDA Issues Safety Advice for Cardiac Device Over Hacking Threat
And even more recently….

- **October 2016:**
  - **Johnson & Johnson** reports remote takeover of one-touch *Ping Insulin Pump*

- **January 2017**
  - **St. Jude Medical** releases security patch to Defense Implantable Cardiac Defibrillator (pacemaker) device
Is there a need for the public policy community to come up to speed as quickly as the technologists, and Define Norms for Connected Medical Devices?
IOT Norms: Standards, Regulation & Law

- **Basic Principles:** A crime is still a crime, even if the instrument is an implanted cardiac defibrillator...
- **Criminal use of a connected device: no need to define a new “crime”**
  - IOT is no different from the advent of Wireless or the Cloud to the “Cyber Ecosystem”, in that 'bad behavior' is still bad behavior, irrespective of the technological nuance.
    - (DISTINGUISH CAPACITY TO DETECT AND FORENSICALLY SUPPORT PROSECUTION—THAT MAY BE “NEW”)
  - Exception where the specific technology materially changes the risk and requires redefining an element of the offense:
    - e.g. If use of a “connected medical device” to commit a battery on a person is substantively different from other batteries using a “weapon”, because act may not be detectable; or the criminal is less detectable

- **Civil Liability for improper design, manufacture or use of a connected device**
  - As with Wireless devices and Cloud, civil liability for reckless design or use of an IOT device may add a new basis for legal liability, determined in a law suit but compensated by new insurance products
  - Changes evidenced in sector best practices statements and industry standards, not law

- **Relation to Federal regulation**
  - Example: connected medical: FDA Conducts pre-market and post market assessment, certification for connected medical devices
  - 2015 *Wyndham Hotels* decision establishes obligation on data custodian to use reasonable security to protect consumer data; may become principle on broad economy-wide duty of wired steward to customer, enforced by FTC “unfair consumer practice” provisions of Section 5 of FTC Act.
Bases of IOT Civil Liability

• **Connected Device production**
  – Emerging new standards of vendor due diligence for manufacture, including
    • **System design**: include consideration of scale, scope and complexity, as well as “hiding in plain sight”
      – Obligation on vendor to appreciate use environment
    – Obligation on vendor to police their own **supply chain**: complex components—microprocessors
      • Emphasis on **assuring security, integrity**, rather than merely identifying defects
      • Exception: faulty firmware or other embedded software.
        – Security Opacity of software requires extensive, extraordinary testing.
    • **Sources**: Industrial Internet Consortium, and individual sectors (e.g. HL7/HIMMS for medical devices)

• **Device use**
  – Obligation on user entity to train and police service provider/user
  – Customer obligation, via contract, to police their own supply chain
  – Insiders are continuing source of risk, liability and thus require due diligence
  – Burden on user/provider to qualify personnel deploying devices
    • E.g. in health care, nurses, specialty therapists, and other staff engaged in direct contact/operation of connected medical devices in the course of patient care
Where do the risks lie?
Bases of Medical Device Liability include:

- **Patients**
  - Physical Harm
  - Emotional Distress
  - Privacy (HIPPA disclosure violations)
  - Economic loss

- **Providers and Vendors**
  - Financial risk: legal liability
  - Business reputational risk/brand
    - Medical malpractice
…and who might be liable?

- **Parties in Interest (“stakeholders”) and sources of risk**
  - **Providers:** Patients, 3rd Party Care givers, Device vendor/service provider,
    - Varies by venue-Self-administered, home, clinic, in-patient facility
    - Physician: primary care, specialist, ancillary (anaesthesia; consultant
  - **Technology:** vendor, component manufacturer, 3rd party provider to venue
  - **Consumables:** drugs, fluids, reagents, dyes

- **Theories of Liability**
  - Distinguish *contractual* Responsibility from legal Accountability
  - **Medical Device Amendments of 1976:** assigning financial accountability irrespective of provable legal responsibility
  - FDA/HHS Pre-, Post- Market approvals:
    - Efficacy, safety IN NORMAL USE
Theories of Liability for defective Medical Devices

1. Privacy/HIPPA unconsented access
   i. Data Loss due to "breach"
   ii. Failure to meet test of "data stewardship"
   iii. FTC/ Wyndham lack of cyber security as an unfair or deceptive consumer practice (§5 FTC Act)

2. Breach of contract

3. Unjust enrichment

4. Bailment (of valuable data)
## Summing up for Medical Devices

<table>
<thead>
<tr>
<th>Harm</th>
<th>Source of remedy</th>
<th>Legal theory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy &amp; Data security Losses</td>
<td>HIPPA, State privacy statutes</td>
<td>Statutory/strict liability</td>
</tr>
<tr>
<td>Bodily injury/Physical Harm</td>
<td>Tort/Contract</td>
<td>Med Mal/Negligence/Breach</td>
</tr>
<tr>
<td>Economic harm</td>
<td>No, unless more than $ loss</td>
<td>“Data as an Asset”</td>
</tr>
</tbody>
</table>
Federal Environment

• **Unhelpful precedent from Data Breach**
  - 6 efforts date to 2006; default to state legislation

• **2015 Cybersecurity Act**
  - HHS Mandate to examine cyber requirements of health device vendors & clinical users

• Health: Sole sector identified for remediation, but
  - No provisions for “connected medical devices”
  - Pending **HHS Task Force Report on Medical Device Cybersecurity**
    - Focus likely to be on security of networks
Rolling these up: New Theories of Liability to Account for Connected Medical Devices

- **IoT Opens New Avenues of Risk Generally**
  - “Big Data”: interpolation/aggregation of specific information about a patient, or a disease, or a cluster
  - Value to collector, but may be criminal under HIPPA
  - Economic Harm to Data Asset
    - Arises from Intentional Act of Defendant a DATA “EXPLOIT”), or
    - Breach of Duty of stewardship over valuable data

- **BUT FOR MEDICAL DEVICES, perhaps, a HIGHER DUTY of CARE?**
  - Even economic harm alone recognized: “patient data” is special data, with special value
    - Losses from:
      - storage device failure (‘Aurora’ rotating media),
      - second order effect physical harm to patient when data is lost/corrupted,
      - deploying entity (clinic, lab)
      - indemnifying insurers or self insurers
Implementing the “higher duty” argument: should the economics be captured in statute?

- Recovery in Negligence is difficult if vendor and provider have done “something/anything” to meet duty of care
- More direct route to recovery is strict liability, such as from statutory liability
  - No need to establish “data” privity; little risk of $0 recovery
  - But, often, multiple defendants, complex, class action

- Liability theories to be embedded in state acts to protect patients:
  i. Design defect—unreasonably dangerous product
     Defective components, open source firmware, network failure, insufficient access security
  ii. Failure of Security: exploit or attack succeeded: *res ipsa*
     Explicitly extend Wyndham “vendor” duty to Connected Medical Devices
  iii. Technology Error or Omission: insurable interest?