Disruptive Health Technologies - The Impact on Privacy & Security
Panel Session Agenda

- Introductions
- Disruptive Health Technologies
- Securing “Disruptive” Healthcare
- Enhancing Privacy in High Tech Healthcare
- Panel Q&A Session

Moderator: Howard Waldner, CHE & Fellow
Setting the Stage -
Disruptive Health Tech

Karina Guy, MAS, PMAHI, CISSP, CISA, CIPP/C
Partner, Advisory Services
KPMG Canada
“The term ‘disruptive’ is used in business and technology literature to describe innovations that improve a product or service in ways that the market does not expect, typically first by designing for a different set of consumers in a new market and later by lowering prices in the existing market. An innovation that is disruptive allows a whole new population of consumers [at the bottom of a market] access to a product or service that was historically only accessible to consumers with a lot of money or a lot of skill.”

Disruptive Healthcare Technology Institute, Carnegie Mellon University
People Trends
- Provider-side democratization of medical technologies and health information technologies
- Drive toward patient-centered care, inter-provider collaboration and patient self-management
- Population advocacy

Process Trends
- Identification of predictive patterns in clinical sub-population requiring large-scale clinical trials and research
- Genomic information systems
- Standardized biobanking (organs, tissue)

Technology Trends
- Rapid commercialization of, and access to health management technologies
- Wearables and convergence of multiple disruptive technologies
- Connected communities
The Convergence of Privacy and Medical Ethics

- Increased demand for medical anonymity
- The resurgence of “self ownership”
- Autonomy of healthcare decisions
- Pseudonymity “in community”
- Provider conscience clauses
- Medically unhealthy lifestyles
- Genetic discrimination
- Ethics of concealment
“Several national governments – for example, in the United States, Australia and a number of European countries – have taken legislative action to address genetic discrimination. While Canadian human rights laws, insurance laws and privacy laws do contain provisions that seek to minimize unjustifiable discrimination and prevent improper access to or use of personal information, at present no laws in Canada provide specific protection against genetic discrimination.”

Library of Parliament Research Publications
Julian Walker, Legal and Social Affairs Division
September 2014
Securing “Disruptive” Healthcare

Shanti Gidwani RN, MSN, MHA, CHE
National Sr Director, Healthcare
Cisco Systems Canada
Security Challenges

- Digitization and Changing Business Models
- Dynamic Threat Landscape
- Complexity and Fragmentation
- Talent Shortage
Complex Challenges for Healthcare

BYOD
50%+
of hospitals are using smartphones or tablets

PHI Data Access
69%
of clinicians are using both a desktop/laptop and a smartphone/tablet to access data

Compliance
138%
the increase in HIPAA data breaches from 2012 to 2014

Breach
54%
of breaches remain undiscovered for MONTHS

Source: Ponemon Research: June, 2015
“Thousands of 'directly hackable' hospital devices exposed online”
“Hackers make 55,416 logins to MRIs, defibrillator honeypots”
Motivated Threat Actors Behind Breaches

<table>
<thead>
<tr>
<th>Type</th>
<th>Avg Payout</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medical Identity Theft</td>
<td>$20,000</td>
</tr>
<tr>
<td>Regular Identity Theft</td>
<td>$2,000</td>
</tr>
<tr>
<td>Social Security</td>
<td>Ave. $1~</td>
</tr>
<tr>
<td>Credit Card Data</td>
<td>$0.25-$60</td>
</tr>
<tr>
<td>Bank Account Info</td>
<td>$1000+ depending on account type and balance</td>
</tr>
<tr>
<td>Full Identity Profile</td>
<td>$500~</td>
</tr>
<tr>
<td>Medical Record</td>
<td>$50+</td>
</tr>
<tr>
<td>Health Insurance Credential</td>
<td>$20+</td>
</tr>
</tbody>
</table>

Source: EMC
You Can’t Protect What You Don’t See

60% of data is stolen in HOURS

85% of point-of-sale intrusions aren’t discovered for WEEKS

54% of breaches remain undiscovered for MONTHS

“51% increase of companies reporting a $10M loss or more in the last 3 YEARS”

“A community that hides in plain sight avoids detection and attacks swiftly”

- “Cisco Security Annual Security Report”
Healthcare Specific Security Measures

- Need to **ACCESS** information whenever and wherever by clinicians
- **AUTHENTICATION** to patient records must be **FAST**
- Movement towards **CLOUD APPLICATIONS** expands security risks
- Multitude of **MEDICAL DEVICES** – all connected and all must be secured (EKGs, Heart Monitors, Medicine Cabinets, implants, etc.)
- Use of **MOBILE DEVICES** and **BYOD** dissolves the network perimeter
Today’s Security Access Scenarios

- Remote Physician Clinic
- Clinician PHI Access
- Bring Your Own Device Mobility/Medical Devices
- Patient Experience/Vendor Support/Guest Services
- Virtual Physician

Connected Health Infrastructure—Security Architecture
Fundamental Questions about Connected Devices:

1. Do the devices store and transmit data securely?
2. Do they accept software security updates to address new risks?
3. Do they provide a new avenue to unauthorized access of data?
4. Do they provide a new way to steal data?
5. Do they connect to the institution's existing IT infrastructure in a way that puts data stored there at greater risk?
6. Are the APIs – through which software and devices connect – secure?
Promoting Cybersecurity Best Practices

Framework covers all three
Threat Centric Security Model

Aligning with the Framework Core

Before
- Discover
- Enforce
- Harden

During
- Detect
- Block
- Defend

After
- Scope
- Contain
- Remediate

Identify | Protect | Detect | Respond | Recover
Visibility and Control Inside Your Network

Before They Attack

During The Attack

After Compromised

Network as a Sensor

Network as an Enforcer
Are you ready?

- Threat-Centric Security
- Cross Functional
- Rising Healthcare Breaches
- End-to-End
- Expanding Security Capabilities
- Proactive Security
- Leverage Current Investment
- Security Integration
- End-to-End
- Mobility Explosion
- Security Everywhere
Enhancing Privacy in High-Tech Healthcare

Khaled El Emam, PhD
Chief Executive Officer
Privacy Analytics
Information garnered from every patient will allow us to learn and to accelerate progress in treating patients. Achieving this goal will require clinicians to have a robust quality monitoring system, the means to collect and analyze data from all patient encounters, and the ability to learn from every one of them, in order to deliver high-quality care to each patient.
Not only:

• the use of evidence at the point-of-care: on-line guidelines, drug interactions, electronic references

• the integration of patient data across multiple settings over time (e.g., hospital, community clinic, and pharmacy) and making that integrated view available to providers at the point of care

• Matching eligible patients with ongoing clinical trials

But also:

• The use of historical data from all patients to make care decisions
Learning from Data & Managing “Similar Patients”

Learnings from Data:
• Integrated data on treatments and (short and long term) outcomes can be queried at the point of care
• Produce reports on the treatments received and prognosis of other similar patients – up-to-date learning from previous experiences

Managing “Similar Patients”
• Matching can be done on multiple variables, including demographics, disease state, treatment history, and genomic information
This information can be pulled automatically from the electronic medical record of the patient
CancerLinQ will organize the explosion of information into usable knowledge, personalized for each and every patient.

Source: Cancerlinq.org
ASCO Cancer LINQ De-Identification

Data Sharing Portal

De-identification Engine

EMR Systems

Big Picture Data Set

Special Request Data Sets

Risk Profiled De-identification

PHI

Anonymous Data
Managing Re-Identification Risk
Managing Re-Identification Risk

[Graphs showing the relationship between uniqueness and characters in postal code for different trace durations (1-11 years)]
De-identification at Scale

Assess Risk
- [ ]
- [ ]
- [ ]
- [ ]

Classify Variables
- Age
- Gender
- Admission

Map Data

Original Data

Automated Anonymization Engine

Anonymized Data
Panel Q&A

Moderator: Howard Waldner