Terry Ziemniak
Assistant Vice President and CISO
Carolinas HealthCare System

www.linkedin.com/in/terryziemniak
Overview

• About Carolinas HealthCare System
• Data Protection
• Privacy
• Security
• Comprehensive Program
Who We Are

Carolinas HealthCare System has a unique story to share.Operating as a fully integrated system and connecting and transforming care delivery throughout the Carolinas, our overarching goal is to provide seamless access to coordinated, high quality healthcare – and provide that care closer to where our patients live.

With 39 hospitals and 900+ care locations, the depth and breadth of services results in a full continuum of integrated care including:

• Prevention and general wellness with focus on population health
• Primary care at more than 180 locations
• Specialty care via several nationally-recognized service lines
• Critical care with one of the largest virtual (e-ICU) programs in the nation
• Continuing care including home health, skilled nursing, hospice, palliative care centers, inpatient/outpatient rehab, and long-term acute care hospital
Where We Are
1. Data Protection

• “Ford sells trucks & McDonalds makes hamburgers”
• What is data & why do we want to protect it?
  • Corporate
  • Individual
  • Government
#Privacy

http://keyhole.co/
Data Protection is Important but:

• Private data is everywhere
  – Tracking activities
  – Location
  – Communication
  – Bio Metrics
  – Photos
Data Protection is Important but:

- People readily give up privacy for:
  - Candy
  - Social Status
  - Discounts
  - Wifi Access
  - Cookie
  - Applications
Data Protection is Important but:

- It is hard for users:
  - Complicated
  - Confusing
  - Inconvenient

https://tosdr.org/#
Data Protection is Important but:

- It is complicated/confusing/inconvenient for organizations
  - Simple means of user authentication
  - Wifi
  - Mismanagement of paper records
  - Costly
  - Incentives/disincentives?
Data Protection is Important but:

• Long history of misuse of private data
  – Government
  – Institutions
  – Relations
  – Hackers/Activists
Data Protection is Important but:

- Moving target
  - New data
  - New uses of data
  - Unintentional data capture
  - Subject of data has change
  - New regulations
2. Privacy

- “Do people know you are monitoring?”
- Define
  - Physical, informational, decisional
- Control
  - Collecting
  - Amending
  - Deleting
  - Accessing
  - Sharing
Examples

- Target shopping
- Google Ads
- Gathering of DNA
- Sewers
- Posthumous access
Right Level of Privacy

• Information
• Subject
• Personal Preferences
• Mandates
• Relationship
  – People (students, parents, spouses, employees, patients)
  – Institutions (school, employer, media, government)
As an Institution we must ask

- What level of privacy is appropriate?
- How do we manage?
- How do we enforce it?
- How do we measure successful program?
3. Security

• “Something happened”
• Define
  – Manage risk
  – CIA AAA
• Controls
Multifaceted Security Program

People - Process - Technology

- Awareness
- Security Operations
- Compliance
- Investigation
- Data Protection
- Assessment & Consulting
- Trends & Strategy
- Policies & Standards
- Auditing
- Incident Management
- Disaster Prep
- Log Management
- Vulnerability Management
- Tech Controls
- Risk Management
- Policies & Standards
- Tech Controls
- Risk Management
Examples

- Refrigerator
- Android phone
- Cars
- Phishing
- Easiest way to hack a password.
Right Level Of Security

- Data Architecture
- Business Support
- Mandates
- Risk management
As an Institution we must ask

• What level of security do we desire?
• Which framework?
• How do we enforce it?
• What does a good program look like?
4. Protection

• “Ashley Who?”

Hello [redacted], you don't know me but I know you very well. As you likely know, the Ashley Madison website was hacked a little while back and in the process some personal information from tens of millions of their clients was compromised. As scary as that sounds, most of their families will never find out. First, they would have to actively seek out the information. Second,

So here is what I did when [redacted] did not pay up by the deadline. I of course anonymously contacted his wife, [redacted] and told her about [redacted]'s membership on Ashley Madison and told her how to confirm it for herself. But I didn't stop there. I also contacted [redacted]'s work colleagues. I also contacted his daughter. And his daughter's boyfriend. And I contacted several of his superiors, peers, and subordinates at [redacted].

You see, [redacted] if you don't comply with my demand I am not just going to humiliate you, I am going to humiliate those close to you as well.

Then there was another man to whom I gave the same letter and he chose to pay. I'll call him “Mr. Wise”. No, that isn't his real name. I am not going to share any of his information with you or anyone else. Ever. You see, HIS secret is safe with me. And he will never hear from me again.

The only real question you need to ask yourself is whether you want me to treat you like [redacted] or like “Mr. Wise”. That choice is completely yours.

If you do not wish me to destroy your life then send $2000 in BITCOIN to the Receiving Bitcoin Address listed below. Payment MUST be received within 10 days of the post marked date on this letter's envelope. If you are not familiar with bitcoin, read the attached “How-To” guide. You will need the below two pieces of information when referencing the guide.

[redacted] was still able from there works for a named [redacted] though she goes by [redacted]. He has a lovely college-aged daughter
## Protection: Privacy vs. Security

<table>
<thead>
<tr>
<th>Issue</th>
<th>Privacy or Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Two factor authentication</td>
<td>Security *</td>
</tr>
<tr>
<td>Sharing flu outbreak info with CDC</td>
<td>Privacy *</td>
</tr>
<tr>
<td>Annual recertification of partner access rights</td>
<td>Security *</td>
</tr>
<tr>
<td>Required logging when sharing research data</td>
<td>Privacy *</td>
</tr>
<tr>
<td>Department use of Google Drives for confidential data</td>
<td>Privacy &amp; Security</td>
</tr>
<tr>
<td>Protecting staff from identity theft</td>
<td>Privacy &amp; Security</td>
</tr>
<tr>
<td>Detecting illegal on-line activity</td>
<td>Privacy &amp; Security</td>
</tr>
</tbody>
</table>
Protection

• Privacy
  – Articulate rules
  – Per data set, per context

• Security
  – Enforces via controls
  – Per system, per business process

• Privacy and security support business mission.
  – Rules of road & Brakes

• Program
## Data Protection Program

### Components

<table>
<thead>
<tr>
<th>Privacy</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory</td>
<td>Auditing</td>
</tr>
<tr>
<td>Guidance</td>
<td>Assessment</td>
</tr>
<tr>
<td>Expertise</td>
<td>Execution</td>
</tr>
<tr>
<td>Training</td>
<td>Policies</td>
</tr>
<tr>
<td>Controls</td>
<td>Authority</td>
</tr>
<tr>
<td>Incident Mgmt</td>
<td>Investigation</td>
</tr>
<tr>
<td>Framework</td>
<td>Reporting</td>
</tr>
<tr>
<td><strong>Driver</strong></td>
<td><strong>Statement</strong></td>
</tr>
<tr>
<td>------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Business</td>
<td>Provide remote access to medical records</td>
</tr>
<tr>
<td>Privacy</td>
<td>Policy states that we restrict access.</td>
</tr>
<tr>
<td>Security</td>
<td>Mechanism to identity and authenticate users on website.</td>
</tr>
<tr>
<td>Business</td>
<td>Staff wants to use share research data</td>
</tr>
<tr>
<td>Security</td>
<td>How secure does this need to be?</td>
</tr>
<tr>
<td>Privacy</td>
<td>Provides input into risk assessment</td>
</tr>
<tr>
<td>Business</td>
<td>Send protected health information to partners</td>
</tr>
<tr>
<td>Privacy</td>
<td>Detect misdirected medical information</td>
</tr>
<tr>
<td>Security</td>
<td>Accomplished this via data loss prevention tool</td>
</tr>
</tbody>
</table>
Privacy and Security: Cautions

- Immature security can impact privacy
- Immature privacy can impact security
- Robust security can impact privacy
- Robust privacy can impact security
Privacy and Security: Differences

- Non electronic
- Stakeholders
- Privacy issues
  - Social media
  - Destruction of paper records
- Security issues
  - On premise solution versus cloud
  - Do we allow consumer devices access?
Build to Grow

• Future Considerations Privacy
  – Growth of data capture
  – Growth in value of data
  – Changing attitudes
  – Data never goes away

• Future Considerations Security
  – Internet of Things (IoT)
  – Consumer technology
  – Big data

• Robust data protection
Data Protection