The Evolving World of Privacy and Security

Kirk J. Nahra
Wiley Rein LLP
Washington, D.C.
202.719.7335
KNahra@wileyrein.com
@kirkjnahrawork

(May 20, 2015)
My Presentation Today

- Big Data has become a hot buzzword in many areas
- Healthcare is a key component of this debate and discussion
- The world of health care data – from a regulatory perspective – is about to change, maybe dramatically.
- I’ll focus on the big development – the debate about “non-HIPAA” healthcare data and what it means for all health care data users and the future of health care privacy (and perhaps overall privacy)
The “next generation” HIPAA issue

- HIPAA has always been a limited scope privacy/security rule
- It applies to healthcare information only where a covered entity is involved.
- Accordingly, there always have been gaps where various entities collect or maintain health care data but are not covered by the HIPAA rules.
The biggest “next generation” issue

- What is “outside” of HIPAA is growing
- Web sites gather and distribute healthcare information - ranging from commercial web sites (e.g., Web MD) to patient support groups.
- Significant expansion of mobile applications directed to healthcare data or offered in connection with health information
- Recent announcements from Apple and Google have expanded this large and growing area.
The Reaction

• It is clear that there is significant concern, from the Federal Trade Commission, privacy advocates and others, about how this “non-HIPAA” health data is regulated.

• Julie Brill - this development involves “health data flows that are occurring outside of HIPAA and outside of any medical context, and therefore outside of any regulatory regime that focuses specifically on health information.”
Big Data Implications

• Much of the “Big Data” discussion is outside of the context of health care, BUT

• there is a wide variety of health care information (both HIPAA regulated and not) that is being scrutinized in the context of Big Data

• and there is a growing range of “Big Data” activities being conducted by healthcare entities, again both in and out of HIPAA.
More “next generation” issues

• An emerging (and related) issue - bringing “outside” HIPAA information “inside” HIPAA

• CEs are gathering all kinds of data about their patients/customers/insureds from outside the health care system and using it for “health care purposes”
Recent Headlines

• Bloomberg - “You may soon get a call from your doctor if you’ve let your gym membership lapse, made a habit of picking up candy bars at the check-out counter or begin shopping at plus-sized stores.”

• New York Times - Health plan prediction models using consumer data from data brokers (e.g., income, marital status, number of cars), to predict emergency room use and urgent care.
More from the FTC

Commissioner Brill (from a recent speech)

• Then the question becomes, though, if we do have a law that protects health information but only in certain contexts, and then the same type of information or something very close to it is flowing outside of those silos that were created a long time ago, what does that mean? Are we comfortable with it? And should we be breaking down the legal silos to better protect that same health information when it is generated elsewhere.
What’s Next?

• The debate about “non-HIPAA” healthcare data is not going away
• There is too much data being used by too many people in too many risky contexts
• Therefore . . .
Tentative Predictions

• This HIPAA/non-HIPAA issue is not going away
• Lots of pressure from many fronts to “do something” about this non-HIPAA health care data
• There will quickly be debate and proposals about regulating this non-HIPAA data
Tentative Predictions

• First issue will be whether to regulate “like HIPAA” or do something else
• This will be an extended and contentious debate
• We are a long way from an agreement/consensus on any of these principles – other than the growing consensus that there is a need for something.
Tentative Predictions

• 3 Main Options
• Something specific for this non-HIPAA health care data
• Something that covers all health care data (a “general” HIPAA)
• A broader overall privacy law (with or without a HIPAA carve-out)
Suggestions

- Understand where your company fits into this debate
- Think about your views on how this should evolve
- Think about the business implications of the various choices
- Think about your role (if any) in the debate
Questions?

For further information, contact:

- Kirk J. Nahra
  Wiley Rein LLP
  202.719.7335
  Knahra@wileyrein.com
  @kirkjnahrainwork

- Subscribe (for free) to Privacy in Focus - http://www.wileyrein.com/publications.cfm?sp=newsletters
Cybersecurity and Privacy

The Evolving World

9 of Cybersecurity and Privacy

HITRUST 2015

...And What It Means for YOUR Organization

Michael Parisi
PwC

Caroline Budde
Walgreens

Kirk Nahra
Wiley Rein, LLC
The new reality...
Beyond the enterprise

The Evolution:
• Technology-led innovation has enabled business and care deliver models to evolve
• The extended enterprise has moved beyond technology and patient-provider integration
• Connectivity and collaboration now extends to all facets of business

Leading to:
• An innovative and interconnected world
The new reality...

Technology domain convergence

<table>
<thead>
<tr>
<th>Information Technology</th>
<th>Computing resources and connectivity for processing and managing data to support organizational functions and transactions; such as user workstations, reporting repositories, data warehouses, web applications, etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational Technology</td>
<td>Systems and related automation assets for the purpose of monitoring and controlling physical processes and events or supporting the creation and delivery of products and services; such as EHRs, nurse stations, hospital scheduling machines, drug allocation devices, etc.</td>
</tr>
<tr>
<td>Medical Devices</td>
<td>The healthcare industry includes a unique convergence of operational and consumer technology in the field of medical devices. These systems control physical processes and events supporting the delivery of medical services while being external end-user focused; such as pacemakers, insulin pumps, CPAP machines, etc.</td>
</tr>
<tr>
<td>Consumer Technology</td>
<td>Computing resources and connectivity integrated with or supporting external end-user focused products and services; such as wearable medical devices, Health &amp; Well-Being Rewards sites, etc.</td>
</tr>
</tbody>
</table>

Cybersecurity encompasses all four technology types
The new reality...
Threat actors and the information they target

Adversary

- Nation State
- Hacktivists
- Organized Crime
- Insiders

What’s most at risk?

- PHI, PII, HIPAA, and other regulatory
- EHR, EMR, and Cloud solutions
- CPOE and Mobile EHR
- Emerging technologies and BYOD
- Online Consumer payments and PCI-DSS
- ERA/EFT and Provider Payments
- Fraud and Anti-Money Laundering
- Medical devices
- Physical theft and loss
- Business deals and strategic information
- Patient safety monitoring

**Motives and tactics** evolve and what adversaries target vary depending on the organization and the products and services they provide.

The new reality...
Why target healthcare?

<table>
<thead>
<tr>
<th>Electronic Health Records are changing the information game</th>
<th>The healthcare business model has evolved, creating a dynamic environment that is increasingly interconnected, integrated, and interdependent - necessitating the transformation of your security practices to keep pace.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health records are now worth more than credit cards and SSN</td>
<td>With Financial Services and Retail having long been targets for cyber attackers, the black markets are flooded with credit card and social security numbers; increasing the value of verified health records and identifiers for use in fraudulent access to healthcare as well as identity theft.</td>
</tr>
<tr>
<td>Healthcare, and new medical research, is a focus of developing nations’ economic plans</td>
<td>Several developing nations have targeted existing healthcare technologies, including patient care, clinical improvements, and intellectual property for further “co-innovation” or “re-innovation” in order to jump start their national economic development plans.</td>
</tr>
<tr>
<td>Healthcare is less prepared to handle cyber events than FS and Retail</td>
<td>Traditional healthcare information security programs have long been narrowly-focused and compliance based efforts that have yet to adapt to the emerging and ever-changing threat landscape presented by these advanced threats.</td>
</tr>
<tr>
<td>Cybersecurity is seen as a barrier to patient care</td>
<td>Cybersecurity is not just an IT issue; rather it requires attention and input from key business leaders, including executives, board or directors, legal, media relations, and others.</td>
</tr>
</tbody>
</table>
OCR Audits

• Phase II- The Critical Review
• Revised Audit Protocol
  – Timely & Thorough Security Risk Assessments
  – Effective & On-going Risk Mitigation Plans
  – Breach Notification Procedures
  – Encryption
  – Training and Policies/Procedures
• Expands the OCR’s Reach for Audits
The Evolving World of Privacy and Security

Caroline Budde, Esq.
Chief Privacy Officer Walgreens
HITRUST Board of Directors
May 20, 2015
Legislative & Regulatory Activity

• Consumer Privacy Bill of Rights
• Breach Notification & Security Laws
  – Federal
  – New York
  – California
  – Illinois
Enforcement Is Growing

• Office for Civil Rights
• Federal Trade Commission
• Attorney Generals
• Class Actions