Is Your Compliance Strategy Putting Your Business at Risk?

January 20, 2015
Today’s Speakers

Michael McAlpen
Exec. Dir. of Security & Compliance, 8x8, Inc.

David Leach
Business Communications Consultant, 8x8, Inc.
Mike McAlpen - 8x8, Inc.
Executive Director, IT Security & Compliance

- Business Leader, Global Information Security & Compliance, Visa Inc.
- Senior Director, Hewlett Packard Professional Services Information Security, CIO/CISO Advisory, Enterprise Architecture Practices
- American Bar Association – Science and Technology Law – Information Security & Forensic Committees
- Senior Member ISACA Information Systems Audit and Control Association
- Member, Communications Fraud Control Association (CFCA)
- Member Cloud Security Alliance (CSA)
- U.S. Secret Service Cyber Crime Task Force
- Board member FBI/DHS InfraGard
- Board member Healthcare Information and Management Systems Society (HIMSS)
Health Insurance Portability and Accountability Act

Pre-2013

HIPAA covered any business associate who performed or assisted in any activity involving the use or disclosure of individually identifiable health information, such as third-party administrators, pharmacy benefit managers and benefit consultants.

Enforceable as of Sept. 23, 2013

Under the new regulations, business associate status is triggered when a vendor “creates, receives, maintains or transmits” personal health information (PHI).
Companies Impacted by HIPAA (partial list)

- Healthcare Provider
- Data Storage
- Finance
- Billing
- Consulting
- Administrative
- Tax Advisor
- Legal
- Cloud
- Healthcare Clearinghouse
- Health Plan
# Penalties for Non-Compliance

Enforced by U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR)

<table>
<thead>
<tr>
<th>Violation Category</th>
<th>Each Violation</th>
<th>All Such Violations Annual Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did not know</td>
<td>$100 - 50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Reasonable cause</td>
<td>$1,000 - 50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful neglect, corrected</td>
<td>$10,000 – 50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful neglect, not corrected</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>
HIPAA Impact on Communications

Electronic Personal Health Information (E-PHI) may be contained in any one of these forms.
PCI-DSS Security Breach Fines

- **MasterCard**
  - Level 1 & 2 Merchants
    - First Violation – up to $25,000
    - Second Violation – Up to $50,000
    - Third Violation – up to $100,000
    - Fourth Violation – up to $200,000
  - Level 3 Merchants
    - First Violation – up to $10,000
    - Second Violation – Up to $20,000
    - Third Violation – up to $40,000
    - Fourth Violation – up to $80,000

- **Visa**
  - Level 1 Merchants - $25,000 monthly
  - Level 2 Merchants - $5,000 monthly

Level 1 – >6 M transactions/yr.
Level 2 – 1-6 M transactions/yr.
Level 3 – 20,000 – 1 M transactions/yr.
PCI-DSS Best Practices

If you take credit card numbers, be sure you . . .

- Never store or write down the CVV2 data (card security code)
- All other card information, if stored, must be encrypted and/or tokenized (i.e. number, user name, exp. Date)
- Ideally pass this data through to your card processing vendor, rather than store it
- Auditors will require verification of training & authorization of all parties handling the data
Other Regulatory Compliance

- Any business concerned with data privacy (Energy, Bio-Tech, Hi-Tech, Law Firms, Labor Unions, Construction, etc…)
- FISMA/FedRAMP (local, state, Federal, defense and the 3rd parties supporting them)
- FERPA - Education
- FFIEC – Financial Services
- GLBA – Financial Services
- Data Privacy Regulations in other Countries
World’s Biggest Data Breaches – 30,000+ Records
Other Compliance Best Practices
Develop a Culture of Compliance to Maintain Data Privacy

What auditors look for:

- Separation of duties
- Evidence of training & authorization
- Secure storage practices (data encryption)
- Reputable 3rd party attestation of any 3rd party vendors persistently handling your sensitive data
- Secure policies & procedures in place
- Due diligence practices
Complete, Secure & Compliant Portfolio

- **HIPAA**
  Don't jeopardize your compliance!

- **FISMA**
  Doing business with government?

- **FIPS 140-2**
  8x8 meets strict US government standards.

- **PCI-DSS v3.0**
  8x8 is secure enough for e-commerce.

- **Safe Harbor**
  8x8 complies with US/ELU/EEA Safe Harbor regulations.

- **CPNI**
  8x8 protects customer information.
The Most Secure & Compliant Cloud Communications Provider

**Alliances**

- HIMSS
- NORTHERN CALIFORNIA Chapter
- [Other logos and mentions]

**Compliances Achieved**

- HIPAA
- FISMA
- FCC
- SSAE 16
- OWASP
- [Other logos and mentions]

**3rd Party Compliance Validations**

- IBM
- Deep Water Point
- [Other logos and mentions]
Quality and security similarities

- Deming’s TQM principles turned around the Japanese auto industry
- You can’t inspect-in quality, you must build quality into a product throughout production.
- The same is true for security, it takes time, effort and complete commitment. 8x8 has done this over many years and it is not at all easy for competitors to copy – it will take them years!
What does it take to meet HIPAA Compliance Requirements?

The HIPAA related data in:
1. **Back end systems** -(50 Policies, 150 audit controls, training, physical security, monitoring, Defense in Depth, OWASP Application Security, DR/BCS

2. **Services & Solutions** -(FIPS 140-2 Data In Motion and At Rest Encryption, Authentication, Logging, etc.)

3. **3rd Parties** –(Must meet minimum above standards and sign BAA

4. **Employee HR personnel records** - (Data security Audited annually)

Must be safeguarded by:
1. Physical
2. Administrative
3. Technical

To protect HIPAA related Data:

C. Confidentiality
   1. Integrity
   A. Availability

Customers require 3rd Party Validation:
Ours is from the nationally known HIPAA Security & Compliance legal authority and author, Stephen Wu.
ChenMed Primary Care Provider Turns to 8x8 for HIPAA-Compliant Cloud Communications

- Innovative, physician-led primary care provider; HIPAA compliance a must
- Over 1,400 employees in 38 locations and six states
- Deployed Virtual Office in all locations; completed in under five weeks
- Customer saving more than $5 million over three year period over Cisco on-premises system

Health Data Innovation: ChenMed CEO Briefs President & Top Advisors

Given the complexity of health care reform and the unrivaled success ChenMed has achieved for tens of thousands of Medicare-eligible seniors, President Barack Obama recently met for a second time with ChenMed CEO, Christopher Chan, MD.

The high-level briefing also involved U.S. Health and Human Services Secretary Kathleen Sebelius, U.S. Centers for Medicare & Medicaid Administrator Marilyn Tavenner, White House Deputy Chief of Staff Mark Childress, U.S. Chief Technology Officer Todd Park, and other senior officials.

It was an honor and privilege to brief the President and senior officials at the White House regarding our secrets for achieving amazing health outcomes for seniors, said Dr. Chen. Having these icons of public health care policy express keen interest our best practices, including the truly innovative end-to-end technologies that do so much to improve our patient experience, underscores the value of what we're doing.
Always Secure Communications

- Hardened software
- DDOS protected network
- Encryption
  - Data in motion
  - Data at rest
- End point authentication
- Protected from man in the middle attacks

8x8 Redundant Network (no single point of failure)

Internet or Private Network
Questions?
Additional Resources

• U.S. Department of HHS HIPAA web site
  http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html
  http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitech/enforcementifr.html
  http://www.hhs.gov/web/508/accessiblefiles/checklists.html

• CMS Security Risk Analysis Tip Sheet

• National Institute of Standards and Technology (NIST)
  http://www.nist.gov/ (search for NIST 800-53 Rev.4)

• SANS Institute (security policy guidance & 20 critical security controls)
  http://www.sans.org/ (look for “Policy Template” link)

• 8x8, Inc. compliance web site
  http://www.8x8.com/VoIPBusinessPhoneSystems/ByBusinessSize/Government/Compliance.aspx
Thank you

Contact us: Mike McAlpen
security-compliance@8x8.com