Getting Hip to HIPAA

Protect Your Business from Legal Action and Significant Financial Penalties

May 15, 2014

David Leach
8x8, Inc.

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

The materials presented in the webinar provided by 8x8, Inc. are intended to provide general information on a particular subject or subjects and are not an exhaustive treatment of such subject(s). 8x8, Inc. makes no representations or warranties about the accuracy or suitability of any information in the webinars and related materials; all such content is provided on an “as is” basis. The information contained in these webinars and related materials has been prepared, compiled, or provided by 8x8, Inc. as a service to subscribers and is not intended to constitute legal advice or the rendering of legal, consulting, or other professional services of any kind. Users of these materials should not in any manner rely upon or construe the information or resource materials in these materials as legal, or other professional advice and should not act or fail to act based upon the information in these materials without seeking the services of a competent legal or other professional.
Today’s agenda:

• Almost every major company in the U.S. is affected by HIPAA. Are you?

• What do you need to do about it?
  – Best practices for achieving HIPAA compliance safeguards

• How can 8x8, Inc. help?
Poll
Mike McAlpen - 8x8, Inc.
Executive Director, IT Security & Compliance

- Business Leader, Global Information Security & Compliance, Visa Inc.
- Director, Professional Services Information Security, CIO/CISO Advisory, Enterprise Architecture and IT Service Management practice areas, HP
- Senior Member Board of Directors, International Systems Security Association (ISSA), Silicon Valley
- Past President, Board Advisor, IT Service Management Foundation (itSMF), San Francisco
- Senior Member ISACA Information Systems Audit and Control Association
- Member, Communications Fraud Control Association (CFCA)
- Senior Member Secureworld Silicon Valley CISO Advisory Board
- Original Member Cloud Security Alliance (CSA)
- U.S. Secret Service Cyber Crime Task Force
- FBI/DHS InfraGard
Breach Activity on the Rise in 2014

Who is Phishing for your PHI?

An email arrives in your inbox tomorrow from someone working at one of the large insurance companies. It tells you that someone has attempted to make changes to your information on their systems. It is very specific because it uses your name and says they feel certain it was due to an attempted hack on their company systems, not from something you did. Then, it also asks you to review the information in the document attached to the email. The want to be sure none of your

The Rise Of Medical Identity Theft In Healthcare

If modern technology has ushered in a plague of identity theft, one particular strain of the disease has emerged as most virulent: medical identity theft.
Main Cause of US Data Breaches Over Time
Published in Harvard Business Review, June 2013

Main Causes of Data Breaches Over Time (U.S.)

- Negligence
- Malicious Attack
- System Glitch

SOURCE: PONEMON INSTITUTE AND SYMANTEC, 2013
COST OF DATA BREACH STUDY: GLOBAL ANALYSIS
Per Record Cost, by Industry of US Data Breaches
Published in Harvard Business Review, June 2013

Per-Record Cost of Data Breaches by Industry ($U.S.)

<table>
<thead>
<tr>
<th>Industry</th>
<th>Cost ($U.S.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health Care</td>
<td>233</td>
</tr>
<tr>
<td>Financial</td>
<td>215</td>
</tr>
<tr>
<td>Pharmaceuticals</td>
<td>207</td>
</tr>
<tr>
<td>Transportation</td>
<td>169</td>
</tr>
<tr>
<td>Communications</td>
<td>150</td>
</tr>
<tr>
<td>Services</td>
<td>134</td>
</tr>
<tr>
<td>Technology</td>
<td>129</td>
</tr>
<tr>
<td>Research</td>
<td>125</td>
</tr>
<tr>
<td>Energy</td>
<td>125</td>
</tr>
<tr>
<td>Hospitality</td>
<td>114</td>
</tr>
<tr>
<td>Consumer</td>
<td>113</td>
</tr>
<tr>
<td>Education</td>
<td>111</td>
</tr>
<tr>
<td>Media</td>
<td>103</td>
</tr>
<tr>
<td>Industrial</td>
<td>103</td>
</tr>
<tr>
<td>Public services</td>
<td>81</td>
</tr>
<tr>
<td>Retail</td>
<td>78</td>
</tr>
</tbody>
</table>

Source: PONEMON Institute and Symantec, 2013
Cost of Data Breach Study: Global Analysis

hbr.org
The HIPAA/HITECH Omnibus Rule and What Has Changed
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)

- Covered Entities
- Business Associates
- Their Sub-contractors

... and more
Partial List of Business Associates’ Services

- Legal
- Actuarial
- Accounting
- Consulting
- Management
- Administrative
- Accreditation
- Financial Services
- Data aggregation
- Document shredding
- Physical or electronic data storage or storage services
- Tech support
- Application support
Partial List of Business Associates’ Activities

- Claims processing or administration
- Data analysis, processing, or administration
- Data storage services
- Billing
- Benefits management
- Practice management
- Repricing
- Utilization review
- Quality assurance
- Patient safety activities
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>
Business Cost of IIHI Breach
Becoming HIPAA/HITECH Omnibus Rule Compliant
Establish a Culture of Compliance

Compliance is not an event or checklist, it’s a mindset

- Top Management valued & driven, whole organization involvement
- Establish agreed upon, easily understood policies
- Define and implement procedures, with training & governance
- Be able to provide evidence of compliance to auditors
- Develop controls and procedures that yield sufficient evidence
  - Documented segregation of duty
  - Faxes transmitted using https
  - Logs
  - Training attestations
How 8x8 Can Help
8x8, Inc. is HIPAA Compliant

8x8, Inc. is not in the business of providing HIPAA compliance advice or services. We do offer the following:

- 8x8, Inc. is a HIPAA/HITECH Omnibus Rule Compliant Business Associate
- 8x8, Inc. offers customers a HIPAA Business Associate Agreement
- 8x8, Inc. will inform our customers on how to keep their 8x8-provided services HIPAA compliant
Configuration Recommendations

For Virtual Office/ Virtual Office Pro

• Fax Handling
  – Turn off automatic fax distribution
  – Authorize specific people for handling electronic faxes
  – Use PC and Mac encryption for stored faxes

• Call Recording
  – Turn off automatic call recording

• Fax and Call Recording
  – Make sure all transmissions are transmitted/received via https

• For Virtual Contact Center
  – If sensitive data is stored in CRM, use the built-in APIs to integrate w/ 3rd party CRM partner, such as Microsoft or Salesforce.com

We also offer “data at rest” encryption for customers at an extra cost
Summary and Helpful Resources
Summary

• Determine if your business is subject to HIPAA compliance
  – Does your company, in any way, handle protected health information (PHI)
  – Are any of your partners subject to HIPAA (Covered Entities or Business Associates)
  – Do your communications with partners or customers involve PHI

• If yes, then obtain written BAAs with all your related sub-contractors

• Gather written BAAs from all of your cloud service providers

• Learn more about the HIPAA/HITECH Final Omnibus Rule
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

• 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
Connect with 8x8
For tips, updates and the latest information.

8x8.com  google.com/+8x8Inc
@8x8       linkedin.com/company/8x8
facebook.com/8x8Inc  www.youtube.com/8x8inc

Contact Mike McAlpen – security-compliance@8x8.com
Visit 8x8.com/Social and connect with us today.