Audio Dial-in Info

Please join the Audio Line by Dialing:

Dial-In: 1-877-211-3621

Toll: 1-719-325-2765

Passcode: 277-997-4035

Having difficulty joining the webinar?

Call Brooke Jeske, 314-552-6141

THOMPSON COBURN LLP

TCLE™

TCLE – Cloud Services for Healthcare Providers: Data Privacy and Security Toolkit

January 27, 2016

Conditions of Use/Disclaimer

The purpose of this webinar is to provide news and information on legal issues and all content provided is for informational purposes only and should not be considered legal advice.

The transmission of information from this webinar does not establish an attorney-client relationship with the viewer. The viewer should not act on the information contained in any of the materials or presentation of this webinar without first consulting retained legal counsel. If you desire legal advice for a particular situation, you should consult an attorney.

Recording

The viewer is advised to check the date the webinar presentation was recorded and, where the information presented is time sensitive, to seek out subsequent updates.

CLE Credit

TCLE Cloud Services for Healthcare Providers: Data Privacy and Security Toolkit is preapproved in the following jurisdictions:

- California: 1.00 hour of general credit
- Illinois: 1.00 hour of general credit
- Missouri: 1.2 hour of general credit

Direct all CLE questions and inquiries to:

Monica Velarde 314-552-6525

mvelarde@thompsoncoburn.com

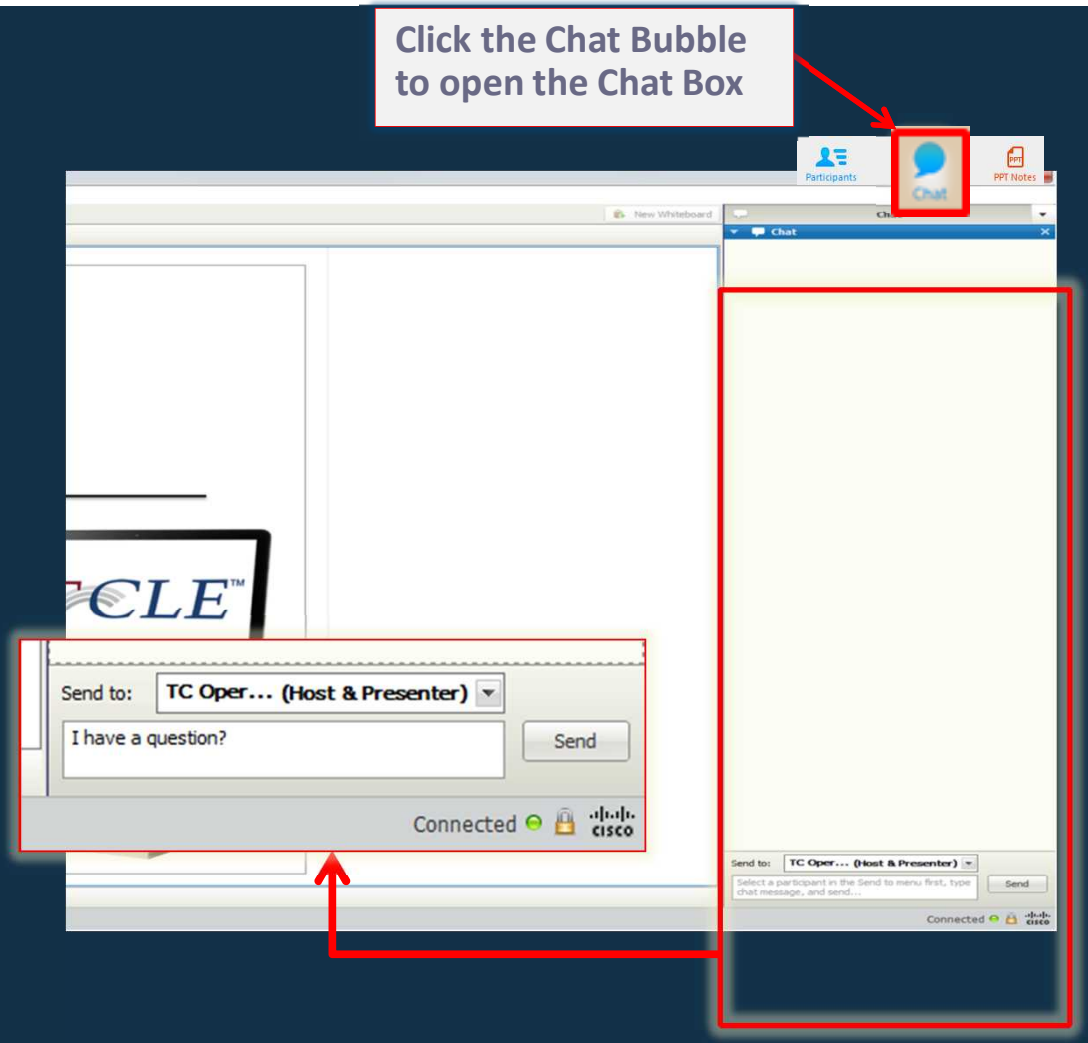
THOMPSON COBURN LLP

TCLE™

Q & A Chat Box

If you have a question, please do the following:

- Click the Chat Bubble to open the Chat Box.
- Type your question in the Chat Box.
- Under the Chat Box in the Sent to area, use the drop down menu to select the name of the presenter.
- Hit the Send button.

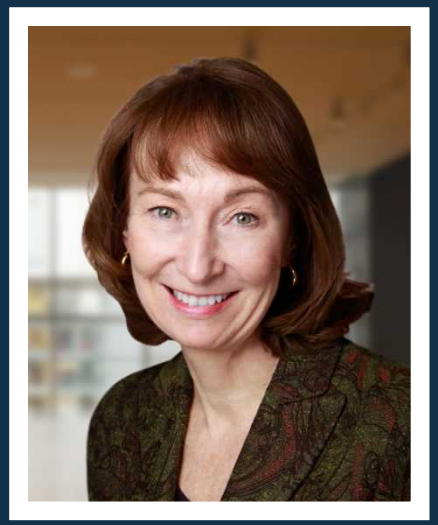


Cloud Services for Healthcare Providers: Data Privacy and Security Toolkit

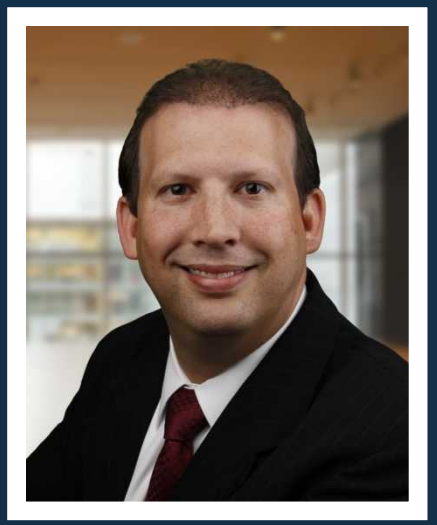
Transaction Risk Mitigation and Implementation Guidance for Healthcare Providers

January 27, 2016

Welcome and Introduction



Joan Lebow



Rob Kamensky

Michelle Skinner

THOMPSON COBURN LLP

TCLE™

Key Points and Tools

- Legal Requirements/Regulatory Regimes
- Enforcement
- Industry Technical Standards/Recommendations
- Third Party Attestations
- Essential Contract Protections
- Qualification of Vendors
- Plan of Action for Providers

Compliance Requirements for Providers

- Health Information Portability and Accountability Act (HIPAA)
  - BA Risk Analysis/Assessment as a contract term
- Replacement of Stage 3 MU with MACRA (Medicare Access and CHIP Reauthorization Act)
- State data privacy and security regimes

Compliance Requirements for Providers

- Medicare Access and CHIP Reauthorization Act MACRA:
  - Will replace Meaningful Use 3
  - Medicare only, physician/clinician only
  - Interoperability requirements for vendors
    - Critical use case approach
    - Federal standards for interoperability 7/1/2016
    - Open APIs
  - Security rules unchanged; focus on exchange of data

Compliance Requirements for Providers

- Cybersecurity Information Sharing Act = CISA
  - No blanket liability protection for Data Breach
  - Liability protection for information/data shared with the Gov't about a cyber-security threat
  - Drafting recommendation: require simultaneous reporting to CE when and if vendor reports as sanctioned by CISA

Compliance Requirements for Vendors

- FTC (Federal Trade Commission)
  - Section 5 of the FTC Act
    - Failure to implement reasonable safeguards to protect the privacy of consumer information
- Federal Communications Commission
  - Federal Communications Act of 1934, 47 U.S.C. section 151
    - Section 201 & 222
  - Net neutrality & Access
  - https://transition.fcc.gov/bureaus/oet/tac/tacdocs/meeting12913/FCC-TAC-Cloud-Sec-Group-Gaps-V14.pdf

FTC Compliance Enforcement Case Study

- Dental Practice Software Provider Settles FTC Charges It Misled Customers About Encryption of Patient Data

- In the Matter of Henry Schein Practice Solutions, Inc.,
  - Charged with false advertisement of compliance with industry encryption standards
    - Dentrix G5, a less complex method of data masking to protect patient data than recommended the National Institute of Standards and Technology (NIST) , misrepresented by vendor
    - Vendor failed to provide t appropriate protection to meet certain regulatory obligations under HIPAA
  - Monetary fine of $250,000
  - 5 Years of future auditing of encryption standards & advertisement compliance
  - Customer Notification
  - "Strong encryption is critical for companies dealing with sensitive health information. If a company promises strong encryption, it should deliver it." Jessica Rich, Director of the FTC's Bureau of Consumer Protection

FTC Compliance Enforcement Case Study

- Henry Schein back story suggests steps providers can take to require disclosure beyond HIPAA requirements to report breach under 45 CFR §§ 164.400-414, and under Federal Trade Commission (FTC) rules pursuant to section 13407 of the HITECH Act.

- https://www.kb.cert.org/vuls/ (Main Site)

  https://www.cert.org/about/ (what the organization is)

  The CERT Division is a trusted provider of operationally relevant cybersecurity research and innovative and timely solutions to our nation's cybersecurity challenges. Through our operationally relevant cybersecurity research, innovative and timely responses to cybersecurity challenges, and broad transition to our stakeholder communities, the CERT Division develops, executes, and evolves a technical agenda that brings unique solutions to cybersecurity challenges that measurably improve the security of the cyber environment.

- https://webcache.googleusercontent.com/search?q=cache:yfmXHhhj71sJ:justinshafer.blogspot.com/2014/05/how-i-beat-henry-schein-and-dentaltown.html%3Fview%3Dsnapshot+&cd=14&hl=en&ct=clnk&gl=us

OCR Compliance Enforcement Case Study

- St. Elizabeth's Medical Center (SEMC)

- SEMC workforce members use of an internet-based document sharing application to store documents containing ePHI of at least 498 individuals….
  - CAP focus on transmission using unauthorized networks and storing EPHI on unsecured networks and devices
- "Organizations must pay particular attention to HIPAA's requirements when using internet-based document sharing applications," - OCR Director Jocelyn Samuels.
- Vendor training of workforce and updates to training modules.
- Contractual requirement of vendor to report data transfers outside of sanctioned environment.

OCR Compliance Enforcement Case Study

- HIPAA Settlement Underscores the Vulnerability of Unpatched and Unsupported Software
- Anchorage Community Mental Health Services, Inc. ("ACMHS")
- Software updates required as made generally available and as required to provide security protection
- Release of patches, updates, **as required to secure application at stated standards**

OCR Compliance Enforcement Case Study

- Data Breach Results in $4.8 Million HIPAA Settlements
- Server exposed to search engines due to failure to adequately follow appropriate safeguards.
- Inventory of devices utilized by parties to develop shared network not performed.
- Shared network firewall not extended to breached server.

FTC Compliance Enforcement Case Study

- *In the Matter of GMR Transcription Services, Inc., Ajay Prasad, and Shreekant Srivastava*
- Decision: August 14, 2014
- Takeaway: Actively oversee your third-party data service provider because you may be at fault for their errors and omissions

FTC Compliance Enforcement Case Study

- **Facts**: GMR provides medical transcription services . It contracted its transcription services to Fedtrans, a third-party vendor that resided out of the country. Fedtrans inadvertently exposed people's medical data maintained by GMR.

- **Findings**: The FTC concluded that GMR's failure to adequately choose, contract with and oversee a data service provider constituted an unfair and deceptive trade practice. According to the FTC complaint, GMR failed to ''adequately verify that their service provider, Fedtrans (out of country vendor), implemented reasonable and appropriate security measures to protect personal information in audio and transcript files on Fedtrans' network and computers used by Fedtrans' typists.''

FTC Compliance Enforcement Case Study

- GMR's specific failings:
  - failed to conduct sufficient due diligence before hiring Fedtrans;
  - failed to contract that Fedtrans adopt and implement appropriate security measures to protect personal information; and
  - failed to take adequate measures to monitor and assess whether Fedtrans employed measures to appropriately protect personal information.

FTC Compliance Enforcement Case Study

- *In the Matter of Genelink, Inc.*
- Decision: May 8, 2014
- Takeaway: You may be liable even if there is no actual breach.

FTC Compliance Enforcement Case Study

- **Facts**: Genelink marketed genetically customized nutritional supplements for treating diabetes, heart disease, arthritis, insomnia, and other ailments. It used third parties to receive, process, or maintain personal information it received from customers.

- **Findings**: The FTC alleged that Genelink's data security practices were lax.

FTC Compliance Enforcement Case Study

- Genelink's specific failings:
  - Failed to implement reasonable policies and procedures to protect the security of consumers' personal information;
  - Failed to require by contract that service providers implement and maintain appropriate safeguards for consumer's personal information;
  - Failed to provide reasonable oversight of service providers;
  - Created unnecessary risks to personal information; and
  - Did not use readily available security measures to limit wireless access to their network.

FTC Compliance Enforcement Case Study

- The cost to both GMR and Genelink:
  - Under the orders, the companies are prohibited from misrepresenting their privacy and security practices.
  - They are required to establish and maintain comprehensive data security programs and submit to security audits by independent auditors every other year for 20 years.
- Will enforcement flow up to providers?

Third Party Attestations

- SSAE No 16, aka SOC (Service Organization Controls) Reports
  - Offered by AIPAC
  - One to Many
  - SOC 2
    - User Management either Operations or Compliance
    - Oversight & Due diligence
    - Detailed system description, controls and tests of controls to determine whether they meet the trust services principles
    - Availability, Security, Confidentiality, Privacy and Processing Integrity
  - SOC 3
    - Any user with need of confidence
    - Limited due diligence & General Confidence
- CSA – STAR Attestation
  - Offered by the Cloud Security Alliance

SOC Reports

Report	Users	Why	Interest
SOC 1/ SSAE 16	Any user with need for confidence in controls relevant to trust services principles, User Auditors	Financial Audit/SOX 404	Controls relevant to user financial reporting
SOC 2	User Management (operations and compliance) Informed Prospects Regulators	Due diligence and oversight Governance, Risk, Compliance Programs	Detailed systems description, controls and test of controls to determine whether meet one or more services principles
SOC 3	Any users with need for confidence in service organization controls	Limited due diligence	General confidence in operating efficiency in controls of trust services principles

SOC System Definition

- Five key components organized to achieve a specified objective:
  - Infrastructure - The physical and hardware components of a system (facilities, equipment, and networks)
  - Software -The programs and operating software of a system (systems, applications, and utilities)
  - People - The personnel involved in the operation and use of a system (developers, operators, users, and managers)
  - Procedures - The automated and manual procedures involved in the operation of a system
  - Data - The information used and supported by a system (transaction streams, files, databases, and tables)

2015 Updates to Scope of SOC

- Must include all System components within the **data lifecycle** for exams addressing Confidentiality or Privacy
  - Creation/Collection
  - Handling/Storage
  - Transmission• Modification
  - Release/Disclosure
  - Processing
  - Use
  - Retention
  - Archival
  - Destruction

Cloud Vendor Technical Standards

- U.S. Department of Commerce
  - NIST (National Institute of Standards & Technology)
    - NIST SP 500-299: NIST Cloud Computing Security Reference Architecture
    - NIST SP 800-144: Guidelines on Security and Privacy in Public Cloud Computing,
    - NIST SP 800-145: The NIST Definition of Cloud Computing
    - NIST SP 800-146: Cloud Computing Synopsis and Recommendations
  - FIPS (Federal Information Processing Standards)
    - FIPS 140-2
    - FIPS 199
    - FIPS 200

Cloud Vendor Technical Standards (con't)

- ISO/IEC
  - ISO/IEC 27017 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services
  - ISO/IEC 27018 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
  - ISO/IEC 27002 Information technology — Security techniques — Code of practice for information security controls
  - ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements
  - ISO/IEC 29100 Information technology — Security techniques — Privacy framework
  - ISO/IEC 29101 Information technology -- Security techniques -- Privacy architecture framework

Key Transaction Goals for Cloud Service

- Cloud Service Agreements
  1. Understand roles and responsibilities
  2. Evaluate business level policies
  3. Understand service and deployment model differences
  4. Identify critical performance objectives
  5. Evaluate security and privacy requirements
  6. Identify service management requirements
  7. Prepare for service failure management
  8. Understand the disaster recovery plan
  9. Define an effective data governance process
  10. Understand the exit process

Provider Risk Mitigation Goals for Cloud Contracts

- Elevate data privacy and governance policies to compliance requirements
- Consider joint liability for compliance requirements with exploration of contract specific insurance and arbitration of allocation of liability and damages
- Shared LOL with caps at differing levels; CFR 160.402 (b) (1)
- Contract for class action litigation defense and indemnity as two separate buckets
- Contract for damages beyond existing coverages as a separate bucket

HIPAA
Flow Downs to BAA's and Subs

- Covered Entity liable for BA breach; risk of civil penalties under the Federal Common Law Rules of Agency
  - For violations, acts or omissions as determined by the Secretary by;
    - Agents
    - Business Associates
      - Workforce Members
      - Sub-Contractors
- Pass through indemnity promises from subs of Vendor

HIPAA
Flow Downs to BAA's and Subs

- The essential factor in determining whether an agency relationship exists between a CE and its BA (or a BA and its subcontractor) is the authority of:
  - A CE to control the BA's conduct in performing services on the CE's behalf.
  - A BA to control the BA-subcontractor's conduct in performing services on the BA's behalf.
  - Federal common law of agency : see Final Omnibus HIPAA Rule Preamble, 78 Fed. Reg. at 5581.
- Basis for Civil Money Penalty
  - 45 CFR §160.402

Just Over the Horizon: Concerns

- FCC: Net neutrality (based on the internet's status as value added carrier) caused FCC to reclassify internet to address regulatory tariffs for internet use
- Section 201; Service and charges: https://www.gpo.gov/fdsys/pkg/USCODE-2011-title47/pdf/USCODE-2011-title47-chap5-subchapII-partI-sec201.pdf
- Section 222: Privacy of customer information https://www.gpo.gov/fdsys/pkg/USCODE-2011-title47/pdf/USCODE-2011-title47-chap5-subchapII-partI-sec222.pdf

Qualifying Vendors Prior to Contract Negotiations

- Use a robust self-reporting tool; see template in our toolkit and convert to ongoing reporting obligation
- Require a central authority to manage integration
- Right to access environment
- Access to event logs
- SLA achievement reports
- Vulnerability testing and reports

Plan of Action for Providers

- Exercise due diligence before hiring cloud service providers;
- Have appropriate protections delineated in cloud providers agreements;
- Team with IT to contract for ongoing surveillance of vendors performance;
- Customize your audit and attestation services to support your security program

HealthIT.gov and More Links

- **Guide to Privacy and Security of Electronic Health Information**
- ISO CLOUD http://www.iso27001security.com/html/27017.html
- http://www.iso.org/iso/isofocus_108.pdf
- **HIPAA Security Rule Toolkit**
- **Cyber Security Risk Assessment Tool**
- **Privacy & Security Training Modules**
- **http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-293.pdf**

TCLE – Cloud Computing Series

TCLE – Cloud Computing 101 – How It Works, What Are Its Risks and What Are Its Rewards

Recording available :
www.thompsoncoburn.com/tcle

TCLE – Medical Mobile Apps: An Overview of the Regulatory Environment

March 16, 2016

Register at: www.thompsoncoburn.com/tcle

Thank You

QUESTIONS

THOMPSON COBURN LLP

TCLE™

Thank You!

Robert Kamensky
rkamensky@thompsoncoburn.com
312.580.2247

Joan Lebow
jlebow@thompsoncoburn.com
312.580.2212

Michelle Ware Skinner
mskinner@thompsoncoburn.com
312.580.5030

THOMPSON COBURN LLP

TCLE™