HEALTHCARE COMMITTEE STRATEGIC PLAN

Co-Chair: Mark Lantzy | Co-Chair: Jacob Butler

September 2018
Indiana Executive Council on Cybersecurity

Healthcare Committee Plan

Contents

Committee Members

Committee Members

Name	Organization	Title	Committee/Workgroup Position	IECC Membership Type
Mark Lantzy	Indiana University Health	SVP/Chief Information Officer	Chair	Voting
Jacob Butler	Parkview Health	Information Security and Compliance Specialist	Co-Chair	Advisory
Mitchell Parker	Indiana University Health	Executive Director, Information Systems	Chair Proxy	Advisory
David Day	Sallie Mae	IDM Manager	Contributing	Advisory
Paul McAninch	Indiana University Health	Director, Information Security and Compliance	Contributing	Advisory
Cliff Campbell	Frakes Engineering	Vice President/General Manager	Full Time	Advisory
Douglas Rapp	Cyber Leadership Alliance	President	Full Time	Advisory
Valita Fredland	Indiana Health Information Exchange	Vice President – General Counsel and Privacy Officer	Full Time	Advisory
Frank Nevers	Federal Home Loan Bank of Indianapolis	Information Security Program Manager	Full Time	Advisory
Leon Ravenna	KAR Auction Services	CISO	Full Time	Advisory
Kim Milford	Indiana University	Lead REN-ISAC	Full Time	Advisory
Paul Baltzell	Mainstreet	VP Information Technology Solutions	Full Time	Advisory

Introduction

Introduction

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) and its mission was continued. With the ever-growing threat of cyberattacks, the IECC has been tasked with developing and maintaining a strategic framework to establish goals, plans, and best practices for cybersecurity to protect Indiana's critical infrastructure. The IECC is comprised of twenty committees and working groups who worked together to develop a comprehensive strategic plan and implementation plans. This implementation plan is one of the twenty specific plans that make up the complete 2018 Indiana Cybersecurity Strategic Plan.

Executive Summary

Executive Summary

- **Research Conducted**
    - We conducted interviews with three people and summarized questions and findings from the Indiana Medical Device Manufacturer's Council (IMDMC) annual meeting, and two discussions with government officials.
        - Jim Routh, Chief Information Security Officer (CISO), Aetna, board member of National Health Information Sharing and Analysis Center (NH-ISAC), and Financial Services Information Sharing and Analysis Center (FS-ISAC) member.
        - Suzanne Schwartz, Doctor of Medicine (MD), Master of Business Administration (MBA), Director, Medical Device Security, U.S. Food and Drug Administration (FDA)
        - Jennings Aske, Juris Doctor (JD), CISO, Columbia/New York Presbyterian Health.
        - Ralph Hall, Leavitt Partners. We spoke with him and summarized findings from the IMDMC annual meeting, including discussions from Eli Lilly, Roche, Hill-Rom, and the Mako Group. Mitch Parker chaired the Cybersecurity panel with members of Lilly, Hill-Rom, Mako Group, and Dr. Schwartz and gave all research notes to the group.
        - Deven McGraw, Former Deputy Director of Enforcement, U.S. Department of Health and Human Services (HHS) Office For Civil Rights.
        - Iliana Peters, Acting Deputy Director of Enforcement, HHS Office For Civil Rights.
        - Nebraska Hospital Association.
        - Josh Singletary, NH-ISAC.
    - We have also utilized several papers and presentations from Mitch Parker and IU Health to provide further research. The papers supplied have 100+ sources each and were submitted as part of graduate school programs.

- **Research Findings**
    - There is high awareness of cybersecurity being an issue in the State of Indiana and nationally.
    - There has been very little practical guidance given to providers that they can use. While HHS has started to give guidance, there is little practical guidance that applies to small to medium size providers.
    - Currently, in Washington, the Health Information Trust Alliance (HITRUST), a private organization, is actively attempting to usurp the NH-ISAC to be the provider of threat intelligence and reporting to healthcare organizations in the U.S.
        - Many providers will not adopt this framework as it is costly and requires full-time investment to be successful.
            - Full HITRUST adoption also requires vendors to buy into it and use the framework.

        - Lessons learned from Department of Defense (DOD). Special frameworks did not work for them (Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) and Department of Defense Information Assurance Certification and Accreditation Process (DIACAP)), and organizations end up falling back to using National Institute of Standards and Technology (NIST) as it is practical and what the rest of the federal government has standardized upon.

- The NH-ISAC is providing all providers with information; however, it is overly technical in nature.
    - While NH-ISAC does have the Threat Intelligence Committee, which is composed of members from the larger providers, and does provide intelligence to other members, it is highly technical in nature most of the time.
- According to the Nebraska Hospital Association, 75% of their hospitals are in rural areas and do not have full-time IT staff.
- According to the American Hospital Association, in 2012, approximately 25% of all hospitals had negative operating margins. The average operating margin was 7.04% for the same time period.
- Electronic Medical Records (EMR) systems require significant initial and ongoing investments. The core EMR system, when purchased initially, requires 25% of the lifetime costs paid up front.
- Even with cloud computing, organizations are required to complete information security risk assessments and document them yearly.
    - There has been a growing perception in healthcare that certain systems that contain protected health information do not need involvement from the formal Info Services e.g. security. This is because the system specific “shadow IT” ends up not waiting for security, doing work, and negating the required security controls necessary to keep them protected.
- Organizations are required, as per the Health Information Technology for Economic and Clinical Health (HITECH) Act, to complete risk assessments of vendors.
- Healthcare organizations are dealing with lower margins, not enough IT staff, and a lack of cohesive guidance.
    - The number of vendor risk assessments that medical device manufacturers have to deal with and the high variety are causing issues with vendors. Jennings Aske is leading an effort to standardize this.
    - While NH-ISAC has the Cyberfit program, which focuses only on applications, licensed by Prevalent, is also costly at $4,000 per assessment. With the number of vendors and applications that a health system can have, if used extensively the program can cost more than staff. Smaller providers typically use the Cyberfit program for a few applications. However, according to Iliana Peters, smaller providers still have to conduct their own organizational risk assessments, even if they do risk assessments of applications.
- The FDA is expecting organizations to include security in their legal contracts. These need to be shared to set global expectations.

  - The FDA understands that current medical device security efforts are losing people over unclear explanations and not listening to customers.
  - According to the FDA, vendors need to be educated on how to present security. Many of the smaller startups are more willing to listen to customers and present a better security plan to their customers. According to Jennings Aske, some large vendors know how to communicate about their own solutions, while many others do not.
    - Standardization and information sharing in this area would provide benefits, according to Jennings, as vendors would be more willing to work with collaborative groups. Binding together groups of organizations, with aggregate market value commensurate with the size of larger medical device companies, is considered incentive enough, indicates Jennings.
  - While researching metrics, the metrics published did not either refer to Bureau of Labor Statistics data on the workforce or only referred to cybersecurity as part of an overall percentage. There is very little empirical data on staffing metrics for cybersecurity as either a subset of IT or healthcare. Only surveys published by Big 4 firms indicate a relative increase in positions, as opposed to a metrics-based approach relative to either organizational size, number of assets managed, or number of applications. The only metrics found specifically related to the number of data breaches themselves.
  - According to Jim Routh, Midwestern organizations are less likely to take advice from national organizations. He spent six years as a CISO in Minnesota and made this observation.
  - The NH-ISAC will be offering discounted endpoint security for all healthcare providers at a very reasonable cost of $10 per machine per year. This addresses a critical need and costs significantly less than other solutions.
  - A number of smaller providers are willing to collaborate. However, not all health systems in Indiana have their security managed locally. St. Vincents, which is part of Ascension, has security managed by an operations center in Troy, Michigan. The issue of collaboration across state lines has to be addressed.
  - According to our research, the practical approaches to implementing cybersecurity need to be communicated better to the medical provider community in a way they can use.

- **Committee Deliverables**
  - Vendor Management
  - Long-Term Education
  - Indiana Threat Intelligence Distribution System

- **Additional Notes**
  - The scope of what we researched indicates that there is a gap between education and practical approaches.

- **References**
  - IU Health Business Associate Agreement and Security Exhibit
  - Interview Notes with Jim Routh, CISO, Aetna, and Suzanne Schwartz, MD, MBA, of the FDA – October 2017
  - *Implementing Secure Cloud Computing in Small to Medium Sized Healthcare Environment*
  - Interview/meeting notes from Indiana Medical Device Manufacturer’s Council Meeting - November 2017
  - *Improving Healthcare Provider Information Security Through the Implementation of Financial Systems Structures and Controls*

Research

Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
    a. Centers for Medicare and Medicaid Services (CMS) has released several guidance documents and programs on cybersecurity.
    b. The Healthcare Information and Management Systems Society (HIMSS) currently offers a comprehensive cybersecurity education program, as does the American Hospital Association (AHA), and American Health Information Management Association (AHIMA). In addition, the National Health Information Sharing and Advisory Center (NH-ISAC) and InfraGard also offers guidance to organizations. HITRUST, which is a for-profit organization, is also popular with many large health systems and payers. They have been providing guidance and a security framework.
    c. Much of this education is focused on either the basics or is aimed at highly sophisticated organizations, which is not the majority of healthcare.

2. **What (or who) are the most significant cyber vulnerabilities in your area?**
    a. Currently, we believe those to be the continuing maintenance and upgrading of systems to protect against new and emerging threats, the abundance of legacy systems, the continuing issues with workflows, the lack of consistent training and education, and the economic pressures causing a de-emphasis on cyber due to having to keep the lights on in many organizations.

3. **What is your area's greatest cybersecurity need and/or gap?**
    a. The need to provide basic education that is relevant to organizations to show them how to protect, as opposed to the constant emphasis on data breaches. CMS has directly indicated that education has been a weak point, and our research shows that the current approach of having one dedicated subject matter expert in each regional office isolates security responsibilities to that one person. Whereas, the institutionalization of security standards that the Federal Financial Institutions Examination Council (FFIEC) has accomplished in finance, is a much more comprehensive cybersecurity program model.

4. **What federal, state, or local cyber regulations is your area beholden to currently?**
    a. We are required to follow the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules, HITECH Act, Stark Act, and a number of state and local laws. In addition, the organizations that have not outsourced their payment processing have to follow Payment Card Industry – Data Security Standards. The organizations that also actively recruit international patients from the European Union (EU) or advertise in the EU must follow the EU General Data Protection Regulation (GDPR).

5. **What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?**
    a. We have highlighted the NH-ISAC Threat Intelligence Committees (TIC) and Cyberfit programs as great examples as for how multiple organizations can work together to identify, classify, and mitigate threats across a large population. We have also discussed how organizations are already self-organizing, specifically with Jennings Aske's work at Columbia/New York-Presbyterian (NYP).

6. **What research is out there to validate your group's preliminary deliverables? This could be surveys, whitepapers, articles, books, etc. Please collect and document.**
    a. We have included two papers written by Mitch Parker, and interviews with Jim Routh, CSO of Aetna; Suzanne Schwartz, MD, MBA, Director of Medical Device Security for the FDA; Ralph Hall from Leavitt Partners at the Indiana Medical Device Manufacturer's Council annual meeting; and Jennings Aske, CISO of Columbia/NYP Health System in New York City (NYC). We have also researched NH-ISAC, Research Education Networking Information Sharing and Analysis Center (REN-ISAC), and a number of other sources.

7. **What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**
    a. They are currently utilizing the same sources we are and also self-organizing as part of emergency management to address these issues. This self-organization includes working with NH-ISAC, REN-ISAC, InfraGard, and through contacts in hospital emergency management, including existing regional organizations.

8. **What does success look like for your area in one year, three years, and five years?**
    a. One year – Begin developing a pilot program modeled after NH-ISAC's Threat Intelligence Committees (TICs) to collaborate across multiple institutions to address security issues, and provide a means for healthcare organizations to contact us to report potential issues. Beginnings of a communication plan designed to reach out to healthcare providers.
    b. Three years – Expansion of the program to have more dedicated staff and interaction with providers. More proactive education. Collaboration with other states and organizations such as NH-ISAC, Infragard, and Department of Homeland Security (DHS) to provide cybersecurity awareness.
    c. Five Years – Having this program as part of normal business of the State.

9. **What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?**
    a. There needs to be a concerted effort to reach out to specific medical providers to specifically address what they need to do to increase security. People are very aware of the need for cybersecurity. The specific guidance that they need to be secure has been either too specific or lacking.

10. What is the total workforce in your area in Indiana? How much of that workforce is cybersecurity related? How much of that cybersecurity-related workforce is not met?

a. According to the 2015 U.S. Bureau of Labor Statistics (BLS) statistics, 9.0% of the total workforce in Indiana is in the healthcare sector.

b. There are no clear statistics as to how much of that section workforce is cybersecurity related.

c. IU Health employs approximately 30,000 people. Approximately 550 of which work in IT, which is approximately 2% of the workforce. Of that, 20 staff members are dedicated to cybersecurity full-time, which is approximately 0.07% of the total workforce at IU Health.

d. According to a Frost & Sullivan report, 30% of healthcare hiring managers plan to increase staff by 20% or more, and 9% of managers want to increase hire between 16-20%.

e. According to the May 2017 HealthCare Industry Cybersecurity Task Force report, coupled with the statistics from the BLS 2016-2026 report. The Cybersecurity vacancies for Indiana Healthcare would be around one dedicated Cybersecurity professional for every 10,000 staff with a minim of one.

f. The issue is not cybersecurity jobs, it is getting people to understand cybersecurity and use due diligence.

11. What do we need to do to attract cyber companies to Indiana?

a. Advertise and leverage the educational advantage that Indiana has with IU, Purdue, IUPUI, Rose-Hulman, and Notre Dame. Two of the best and most well-connected Cyber programs in the country are here, and there are already a number of tech companies, specifically Salesforce, taking advantage of that. Facilitating business development and encouraging companies to locate offices and/or staff here based on the availability of top-level graduates, quality of living, and low cost of living would really help.

12. What are your communication protocols in a cyber emergency?

a. We follow the Hospital Incident Command System (HICS) to escalate incidents. We now have coordinated communication with multiple agencies and will follow the same protocols as a standard multi-site incident. Ultimately, a multidisciplinary approach in healthcare is needed that utilizes HICS as patient safety has to be paramount.

13. What best practices should be used across the sectors in Indiana? Please collect and document.

a. Focus on assessing risk and helping people understand what to do to address it. The issue is that we do not focus on the fundamentals and need to treat cybersecurity as part of the business, not just something to address separately. The more we focus on it as a separate discipline, the less we will be able to attack root causes for many of these issues.

Deliverable: Vendor Management

Deliverable: Vendor Management

General Information

1. **What is the deliverable?**
   a. Indiana-focused versions of security education targeted at small to medium-sized providers. Most of the guidance given out by CMS to providers makes the assumption that providers either have an IT staff or someone with the requisite level of expertise within the organization to interpret guidance and give the staff an answer. As part of discovery on several other projects, we discovered that most small to medium sized providers and critical access hospitals do not have the staff needed to implement solutions, and that they have not been educated on what to do.
   b. The goal of this solution is to provide staff at small to medium-sized businesses with the information they need to assess and address risk with their third-party vendors that provide services to the healthcare community. In addition, this will provide education that non-technical staff can use to make better purchasing decisions that improve cybersecurity.

2. **What is the status of this deliverable?**
   a. In-progress; 75% complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
   ☐ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☒ Strengthen best practices to protect information technology infrastructure.
   ☐ Build and maintain robust statewide cyber-incident response capabilities.
   ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☒ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. Providers will be able to make better decisions regarding the security and safety of the products they use and maintain at their organization

6. **What metric or measurement will be used to define success?**
   a. Number of providers utilizing the training.
   b. Number of products purchased/evaluated using these guidelines.

7. **What year will the deliverable be completed?**
   a. 2019

8. **Who or what entities will benefit from the deliverable?**
   a. Small to medium healthcare entities across the State who do not currently receive this type of information or training on purchasing products.

9. **Which state or federal resources or programs overlap with this deliverable?**
   a. This partially overlaps with the work NH-ISAC, REN-ISAC, and Infragard are currently doing. However, they are not reaching the smaller providers or providing targeted training toward the purchasing process.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Infragard, NH-ISAC, REN-ISAC, and the State and Local Government committees. We also plan on working with and sharing this information with other committees.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Infragard, NH-ISAC, REN-ISAC, Indiana Office of Technology (IOT), Indiana Hospital Association (IHA).

12. **Who should be main lead of this deliverable?**
    a. Mitch Parker

13. **What are the expected challenges to completing this deliverable?**
    a. Backlash from vendors who will view this as losing sales.
    b. Communicating this out to the right staff that need to see it.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort

Tactic Timeline

Tactic	**Owner**	**% Complete**	**Deadline**	**Notes**
Webinar	Mitch Parker	10	January 2019	Need a platform to host on for everyone – based off of IU Health training
Indiana Medical Device Manufacturer's Council	Mitch Parker	50	November 2018	Conference Organizer has approved in light of June meeting being cancelled for annual meeting.
October 23 Conference	Mitch Parker	10	October 2018	Will need conference organizers to approve
One-pager documents and materials	Mitch Parker and IECC Healthcare Committee	20	February 2019	Two-factor authentication documents awaiting final review, encryption to be done by this date.

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes

b. **If Yes, please complete the following**

Estimated Initial FTE	**Estimated Continued FTE**	**Skillset/Role**	**Primary Source of Funding**	**Alternate Source of Funding**	**Notes**
0.5	0.5	Marketing / Communications	Indiana IOT	Grant	Need to have someone help with communication and distribution under proper branding

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	**Justification/Need for Resource**	**Estimated Initial Cost**	**Estimated Continued Cost, if Applicable**	**Primary Source of Funding**	**Alternate Source of Funding**	**Notes**
Webinar Platform	Need to effectively communicate out using IOT approved one			IOT	Grant	We do not have data on Indiana state pricing for these services.
Print/web communications	Need to get the message out to stakeholders.					We do not have data on Indiana state pricing for these services.

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. The greatest benefit is being able to reach a number of medical device manufacturers in one place and communicate out requirements. In addition, reaching a large number of providers through communications will also help get the message out about vendor management and improving security.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. We will set expectations with the vendors, many of which are headquartered in Indiana, and are reaching specific market segments that up until last year had been underserved in security communication, specifically the orthopedic device manufacturers. We estimated 0.5 of a full-time IOT employee to address facilitating and managing the communication process, and additional communication/marketing costs for webinars and one-pagers.

b. Providers will be able to make better decisions regarding the security and safety of the products they use and maintain at their organization

19. What is the risk or cost of not completing this deliverable?

a. We will not be able to communicate out security and vendor management information to the providers that need it the most in Indiana.

20. **What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?**
    a. Number of providers utilizing the training.
    b. Number of products purchased/evaluated using these guidelines.
    c. The baseline will be the number of providers we communicate during the month of August 2018.

21. **Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?**
    a. No

22. **Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?**
    a. No

Other Implementation Factors

23. **List factors that may negatively impact the resources, timeline, or budget of this deliverable?**
    a. There may be backlash from vendors who could see this as negatively impacting sales.
    b. There may be backlash from vendors who see this as potential government infringement on their products.

24. **Does this deliverable require a change from a regulatory/policy standpoint?**
    a. No

25. **What will it take to support this deliverable if it requires ongoing sustainability?**
    a. We documented that there will be program management/marketing/communications support needed from the State if we are to succeed in this endeavor.

26. **Who has the committee/working group contacted regarding implementing this deliverable?**
    a. We have spoken with Infragard, NH-ISAC, REN-ISAC, the Indiana Hospital Association, OrthoWorx, and Indiana University (IU).

27. **Can this deliverable be used by other sectors?**
    a. Yes
    b. **If Yes, please list sectors**
        i. State and Local Government, Water/Wastewater, Cyber Sharing, and whoever else wants to use it.

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. We need to notify all medical device manufacturers in the State, and we can use relationships with the Indiana Medical Device Manufacturer's Council to do so. We have reached out to Tory Castor, SVP Government Affairs at IU Health, to help facilitate. We are already speaking with IU and OrthoWorx Indiana.

b. We would also want to use the communication channels available from IOT and the State under their plan and branding.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. We want to keep the brand and messaging tight and consistent across deliverables. Our greatest concern is that there will be mixed messages across the different committees, and we cannot afford to waste time or give an incoherent message to communities that have little time to waste. We need to be coordinated in this effort and that is where we could have the greatest issue.

Evaluation Methodology

Objective 1: Create vendor management resources for healthcare providers by February 2019.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Distribute vendor management resources to eighty percent of healthcare providers by April 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☐ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☒ Qualitative Analysis
☒ Quantifiable Measurement
☐ Other

Deliverable: Long-Term Education

Deliverable: Long-Term Education

General Information

1. **What is the deliverable?**
    a. Indiana-focused versions of security education targeted at small to medium-sized providers. Most of the guidance given out by CMS to providers makes the assumption that providers either have an IT staff or someone with the requisite level of expertise within the organization to interpret guidance and give staff an answer. While working on several other projects, we discovered that most small to medium sized providers and critical access hospitals do not have the staff needed to implement solutions and that they have not been educated on what to do. Most importantly, they do not even know where to report breaches.
    b. The goal of this solution is to give actionable items to these organizations to implement reasonable security solutions and help prevent common security issues with basic targeted education. We have spoken with the Water committee and discovered we had the same issue where most small to medium-sized organizations do not have security staff needed to implement solutions, lacking/no security education, and don't know how to handle breaches.

2. **What is the status of this deliverable?**
    a. In progress; 40% complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☐ Strengthen best practices to protect information technology infrastructure.
    ☒ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☒ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. Providers at all levels will be able to utilize actionable information to protect themselves against emerging threats.
   b. Better community awareness of threats and, more importantly, actionable steps that providers can take to protect themselves using communications they can understand.

6. **What metric or measurement will be used to define success?**
   a. Number of providers utilizing the service and actively protecting themselves.
   b. Number of organizations receiving intelligence (time period comparisons).

7. **What year will the deliverable be completed?**
   a. 2019

8. **Who or what entities will benefit from the deliverable?**
   a. Small to medium healthcare entities across the state who do not currently receive this type of actionable intelligence.

9. **Which state or federal resources or programs overlap with this deliverable?**
   a. This currently partially overlaps with the work NH-ISAC, REN-ISAC, and InfraGard are currently doing. However, they are not reaching to the level we intend to.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. InfraGard, NH-ISAC, REN-ISAC, and the State and Local Government committees. We also will hopefully be working with the Water committee as we share the same challenges.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. InfraGard, NH-ISAC, REN-ISAC, Indiana IOT, Indiana Hospital Association, Indiana Health Information Exchange (IHIE).

12. **Who should be main lead of this deliverable?**
    a. Mitch Parker

13. **What are the expected challenges to completing this deliverable?**
    a. Communicating to the providers and utilizing multiple avenues to do so.
    b. Threat Complexity. Having to deal with multiple threat variants affecting providers.
    c. Bad patches from vendors (Meltdown/Spectre). Red Hat, Microsoft, and numerous other vendors have released bad patches for vulnerabilities. We don’t want to cause machines to malfunction because of non-functional patches.

Implementation Plan

14. Is this a one-time deliverable or one that will require sustainability?

a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Educational Programs	Mitch Parker and IECC Healthcare Committee	50	March 2019	Will be using previously developed content
Webinars	Mitch Parker	50	February 2019	Will be using previously developed content
One-pager documents	Mitch Parker and IECC Healthcare Committee	20	February 2019	Encryption and one other document to be ready by then

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
0.5	0.5	Marketing / Communications	IOT	Grant	Need to have someone help with communication and distribution under proper branding

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	**Justification/Need for Resource**	**Estimated Initial Cost**	**Estimated Continued Cost, if Applicable**	**Primary Source of Funding**	**Alternate Source of Funding**	**Notes**
Webinar Platform	Need to effectively communicate out using IOT approved one			IOT	Grant	We do not have data on Indiana state pricing for these services.
Print/web communications	Need to get the message out to stakeholders.					We do not have data on Indiana state pricing for these services.

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. We will be able to reach an underserved population that traditionally has been ignored by cybersecurity efforts and provide them with information they can use.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. This deliverable will reduce risk and impact by providing targeted communications to a population that historically has not received them. The costs would include a full-time or equivalent FTE to own the program at the IOT level, resources needed for communication (email, website, postal mailings), and the time from committee member institutions needed to craft the messaging. Enforcement will be through the committee chairs and designates working to allocate resources and monitoring contributions.

19. What is the risk or cost of not completing this deliverable?

a. We will continue to have cybersecurity and ransomware attacks that can be easily preventable affecting both patients and providers in this State. Indiana has made national headlines for several ransomware attacks. We need to prevent the numerous small businesses and providers that make up the bulk of our healthcare providers from falling victim to similar attacks.

20. **What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?**
    a. Number of providers utilizing the service and actively protecting themselves.
    b. Number of organizations receiving intelligence (time period comparisons).
    c. We are going to use the number of providers using these in August 2018 as the baseline.

21. **Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?**
    a. No

22. **Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?**
    a. No

Other Implementation Factors

23. **List factors that may negatively impact the resources, timeline, or budget of this deliverable?**
    a. The largest factor would be the necessity of having someone in IOT in place to facilitate getting us this list.
    b. The other major factor is making sure we have enough coverage from members to address covering the news and intelligence sources to develop communications.

24. **Does this deliverable require a change from a regulatory/policy standpoint?**
    a. No

25. **What will it take to support this deliverable if it requires ongoing sustainability**?
    a. We will need a resource within IOT who can work on behalf of the committee coordinating it and making sure information is current.

26. **Who has the committee/working group contacted regarding implementing this deliverable?**
    a. Chetrice Mosley.

27. **Can this deliverable be used by other sectors?**
    a. Yes
    b. **If Yes, please list sectors:**
        i. Water/Wastewater, Cyber Sharing, and State/Local Government.

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. We believe that all other sectors should be informed as we want them to use it as well.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. We should discuss unifying this with other communications that IOT and other agencies put out so that we give a consistent message to constituents.

Evaluation Methodology

Objective 1: IECC Healthcare Committee will create Indiana-focused versions of security education by March 2019.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group

☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Provide Indiana-focused versions of security education to eighty percent of Indiana healthcare providers by May 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☐ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group

☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☒ Quantifiable Measurement
☐ Other

Deliverable: Indiana Threat Intelligence Distribution System

Deliverable: Indiana Threat Intelligence Distribution System

General Information

1. **What is the deliverable?**
    a. An Indiana-focused version of the NH-ISAC Threat Intelligence Committee focused on distributing information to all levels of providers. Based on conversations with several NH-ISAC representatives, as well as representatives from several other organizations, the major issue is that people are aware of threats, but not how to respond to them.
    b. This deliverable would be representatives of larger health systems taking threat intelligence from NH-ISAC, REN-ISAC, and numerous other sources, and providing actionable information that small to medium size providers can use as a checklist to ensure they are protected against vulnerabilities rather than the current system where providers have to interpret the threats themselves.
    c. The current efforts, while valiant, are representative of the issue that internal security services needs to better communicate with other organizations and within the organizations that they belong to.

2. **What is the status of this deliverable?**
    a. Not Started

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☐ Strengthen best practices to protect information technology infrastructure.
    ☒ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☒ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. Providers at all levels will be able to utilize actionable information to protect themselves against emerging threats.
   b. Better community awareness of threats, and more importantly, actionable steps that providers can take to protect themselves using communications they can understand.

6. **What metric or measurement will be used to define success?**
   a. Number of providers utilizing the service and actively protecting themselves.
   b. Number of organizations receiving intelligence (time period comparisons).

7. **What year will the deliverable be completed?**
   a. 2018

8. **Who or what entities will benefit from the deliverable?**
   a. Small to medium healthcare entities across the state who do not currently receive this type of actionable intelligence.

9. **Which state or federal resources or programs overlap with this deliverable?**
   a. This currently partially overlaps with the work NH-ISAC, REN-ISAC, and InfraGard are currently doing. However, they are not reaching to the level we intend to.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. InfraGard, NH-ISAC, REN-ISAC, and the State and Local Government committees.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. InfraGard, NH-ISAC, REN-ISAC, IOT, Indiana Hospital Association, Indiana Health Information Exchange.

12. **Who should be main lead of this deliverable?**
    a. Mitch Parker

13. **What are the expected challenges to completing this deliverable?**
    a. Communicating to the providers and utilizing multiple avenues to do so.
    b. Threat Complexity. Having to deal with multiple threat variants affecting providers.
    c. Bad patches from vendors (Meltdown/Spectre). Red Hat, Microsoft, and numerous other vendors have released bad patches for vulnerabilities. We don’t want to cause machines to malfunction because of non-functional patches.

Implementation Plan

14. Is this a one-time deliverable or one that will require sustainability?

a. Ongoing/sustained effort

Tactic Timeline

Tactic	**Owner**	**% Complete**	**Deadline**	**Notes**
Identify Medical Providers and Healthcare Organizations	IOT/Professional Licensing Agency/State DOH	0	October 2018	We need to have this hosted by IOT or the state government.
Identify participating healthcare organizations	Mitch Parker, Jake Butler	0	October 2018	
Develop Communication Strategy	Mitch Parker, Jake Butler, Frank Nevers	0	October 2018	
Develop initial pilot group	Andy VanZee, Mitch Parker	0	November 2018	
Send initial messages	Mitch Parker, Jake Butler	0	December 2018	
Gather feedback and refine	Team	0	February 2019	
Continue to send messages	Team	0	February 2019	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes

b. **If Yes, please complete the following**

Estimated Initial FTE	**Estimated Continued FTE**	**Skillset/Role**	**Primary Source of Funding**	**Alternate Source of Funding**	**Notes**
1	1	Security/Threat Intelligence	IOT	Grant	We need to have a resource within state government/IOT able to own the program and sustain it on behalf of the committee and maintain web site
0.25	0.25	Provider-side threat intelligence	Participating healthcare providers		We need resources at the providers who can distill this intelligence and craft communications for end users/providers.

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	**Justification/Need for Resource**	**Estimated Initial Cost**	**Estimated Continued Cost, if Applicable**	**Primary Source of Funding**	**Alternate Source of Funding**	**Notes**
Email address	Need a group email to send communications out to			IOT		
Web Site	Need to have a web site to communicate out					
Marketing/Mailing Lists	Need to send initial communications and ongoing large-scale alerts out to providers					

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. Utilizing the resources of the Indiana state government, specifically the Professional Licensing Agency and Department of Health, current medical and healthcare providers can be identified and targeted for specific cyber education. Current efforts alert people there is an issue, but do not provide targeted remediation guidance. The resources of the Indiana state government can be utilized to address a critically underserved group that is not communicated to. As these providers have to register with the State to stay current, we will be able to utilize the maintained lists to target a current group.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. This deliverable will reduce risk and impact by providing targeted communications to a population that historically has not received them. The costs would include a full-time or equivalent FTE to own the program at the IOT level, resources needed for communication (email, website, postal mailings), and the time from committee member institutions needed to craft them.

19. What is the risk or cost of not completing this deliverable?

a. We will continue to have cybersecurity and ransomware attacks that can be easily preventable affecting both patients and providers in this State. Indiana has made national headlines for several ransomware attacks. We need to prevent the numerous small businesses and providers that make up the bulk of our healthcare providers from falling victim to similar attacks.

20. **What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?**
    a. Number of providers utilizing the service and actively protecting themselves.
    b. Number of organizations receiving intelligence (time period comparisons).
    c. The baselines will be the groups signed up or communicated to in August 2018.

21. **Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?**
    a. No

22. **Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?**
    a. No

Other Implementation Factors

23. **List factors that may negatively impact the resources, timeline, or budget of this deliverable?**
    a. The largest factor would be the necessity of having someone in IOT in place to facilitate getting us this list.
    b. The other major factor is making sure we have enough coverage from members to address covering the news and intelligence sources to develop communications.

24. **Does this deliverable require a change from a regulatory/policy standpoint?**
    a. No

25. **What will it take to support this deliverable if it requires ongoing sustainability?**
    a. We will need a resource within IOT who can work on behalf of the committee coordinating it and making sure information is current.

26. **Who has the committee/working group contacted regarding implementing this deliverable?**
    a. Chetrice Mosley.

27. **Can this deliverable be used by other sectors?**
    a. Yes
    b. **If Yes, please list sectors**
        i. Water/Wastewater, Cyber Sharing, and State/Local Government

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. We need to notify the other committees, IOT, and the providers listed. Resources included in the plan for initial mailings and communications.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. We want to make sure that this is being covered under the right branding, and that we work with Indiana state marketing agencies and resources to develop clear and consistent communications.

Evaluation Methodology

Objective 1: Develop a pilot program with three participants of the Indiana Health Cyber Threat Intel Committee by November 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Evaluate pilot program and recommend a sustainability framework model for the state of Indiana to maintain by February 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☐ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☒ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Supporting Documentation

Supporting Documentation

This section contains all of the associated documents that are referenced in this strategic plan and can be used for reference, clarification, and implementation details.

- IECC Healthcare Committee Jim Routh Meeting Notes
- IECC Healthcare Committee Indiana Medical Device Manufacturers Council (IMDMC) Meeting Notes
- IU Health Business Associate Agreement and Security Exhibit
- Lasalle University Implementing Secure Cloud Computing in the Small to Medium-Sized Healthcare Environment
- Temple University Improving Healthcare Provider Information Security Through the Implementation of Financial Systems Structures and Controls

IECC Healthcare Committee

Jim Routh Meeting Notes

October 2017

Jim Routh and Dr. Suzanne Schwartz writeup

10/30/2017

Jim Routh – Aetna CISO -

Questions:

1. What have you found effective with information sharing in FS-ISAC?
    1. NH-ISAC?

The key here has been the Threat Intelligence Committees, TICs, which are made up of the best malware hunters and threat analysts across the member organizations, do the initial triaging and make the determination as to what information to distribute. They specifically look to see if these attacks are targeted, or if they are opportunistic. They then make specific recommendations as to actions to take to protect organizations. It is important to note that these are member organizations.

The TICs help out smaller organizations by giving them specific guidance. This is better for smaller organizations that have 1-2 IT people total.

What has been effective in both the NH and FS-ISAC committees is that they give targeted advice to smaller providers. Many of the NH-ISAC programs, such as Cyberfit, are geared toward smaller providers.

2. What areas have you found for improvement in FS-ISAC and NH-ISAC?

The membership has been growing at 30-40 members a month. However, the issue has been getting members. The major issue has been that HITRUST has been lobbying Congress to be the framework and vehicle of choice for dissemination of threat intelligence. HITRUST is a for-profit corporation attempting to push a framework which many small providers will not adapt. NH-ISAC, on the other hand, is non-profit and is a collaborative of many of the largest health systems modeled after FS-ISAC.

FS-ISAC has significant governmental support, including the states of NY and MA, which mandate membership. NH-ISAC has not gotten the level of support it needs because HITRUST has been lobbying against it to Congress, specifically the House Energy and Commerce Committee.

NH-ISAC is also attempting to provide for smaller medical providers by signing a joint partnership agreement with a next-generation endpoint protection company. This will allow them to provide endpoint protection at approx. $10/computer per year, and is aimed at smaller providers with less than 200 total seats. This is significantly less than other solutions, specifically Microsoft's.

Specifically, the area for improvement is to get organizations to adopt NH-ISAC's information sharing and protection plans, and see the benefit, rather than the intense lobbying effort from HITRUST which is damaging NH-ISAC.

Collaboration is absolutely key. People in the Midwest aren't going to listen to a national organization. They're going to want to collaborate with themselves first. Jim is a former Minnesota resident who worked there for 6 years, which is why he made that statement.

While we have NH-ISAC, the best conduit is going to be Indiana itself.

3. What do you think makes up a good education program?

People are well aware of what cybersecurity is now. They need to know what to do and how to act, and your training needs to focus on that rather than just more awareness. We have the awareness part down. People need to know what to do!

4. How do you best structure security programs to accommodate a high variety of scale?

This is where you have to leverage the ISACs to provide this information and use them to help with distribution

5. Anything else?

We've found that the use of DMARC, which is very simple to set up in Office365, but not in Google, is very effective at stopping Phishing attacks.

You also need to remove the use of the SSN wherever not absolutely necessary. Aetna has cleaned up over 7 billion SSNs and still has 2 years to go on the project. This is a long-term commitment companies need to make.

Bonus – Dr. Suzanne Schwartz – FDA

I interviewed her as part of the Indiana Medical Device Manufacturer's Council panel I am moderating on Nov. 1.

Advice from her:

1. Collaboration is key, especially with medical devices.
2. Cannot address this in a siloed manner at all.
3. There needs to be a balance. You need to pause and listen when presenting, and read the audience. People get lost with acronyms and without explanations.
4. Current medical device security efforts are losing people over unclear explanations and not listening.
5. We need to be proactive and address issues right then and there.
6. We need to have this information in contracts. Those need to be shared to set global expectations.
7. Vendors need to be educated. Some big companies get it, many don't. Many of the smaller startups are more willing to listen.
8. There needs to be two-way dialogue between the vendors and customers to set the right level of expectations.

IECC Healthcare Committee

Indiana Medical Device Manufacturers Council (IMDMC) Meeting Notes

November 2017

Notes from IMDMC Meeting:

1. I spoke with Ralph Hall, Partner, Leavitt Partners. He is friends with our General Counsel, Mary Beth Claus, and worked with her for a number of years.
2. Ralph has indicated that there is a lack of federal standards for medical device cybersecurity.
3. The current congressional gridlock has caused any meaningful legislation to have no chance.
4. Medical device manufacturers, due to the lack of federal standards, are trying to rely on state standards.
5. At this point there are upwards of 20, and the companies are having a very difficult time keeping up. There is no agreement on what standards to follow.
6. From me, not Ralph - The EU is doing a better job with GDPR, and may end up being the de facto standard with ISO in light of the current situation.
7. Medical Device Vendors are developing their own standards and are willing to work with companies on them. They are cooperating. Best examples I can give are the collaboration between Merck and Eli Lilly, and the current proposed research collaboration of IU/IU Health/Eli Lilly/Cisco we are working with Von Welch on. I can also give the examples of BD and IU Health, and GE Healthcare and IU Health.
8. NH-ISAC is ineffective at best. Despite the best efforts of Jim Routh, the information they give out is often duplicative and does not show true direction.
9. If we do this, we need to do it ourselves. However, this does not solve for the other 49 states. If we do this, we may do this and set a true example for others.
10. We can take advantage of what NH-ISAC has to offer, but we need to make this accessible for Hoosiers.

IU Health

Business Associate Agreement and Security Exhibit

February 2017

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("BAA"), by and between _______________________ ("Business Associate"), of ________________________________, and _______________________________ and Indiana University Health, Inc. (individually and collectively referred to herein "Covered Entity"), of _________________________ Indiana, _________ is made and effective conterminously with the parties' service agreement ("Service Agreement"), to which it is attached.

RECITALS

WHEREAS, Business Associate agrees to provide certain services ("Services") for or on behalf of Covered Entity in accordance with the parties' Service Agreement; and

WHEREAS, in connection with those Services, Covered Entity plans to disclose to Business Associate certain Protected Health Information ("PHI" – used to refer specifically to data controlled or owned by Covered Entity), including electronic PHI or ePHI, (as defined in 45 C.F.R. §160.103) that is subject to protection under the Health Insurance Portability and Accountability Act of 1996, Public Law No. 104-191 ("HIPAA") Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule", 45 C.F.R. Parts 160 and 162 and Part 164, Subparts A and E); and 45 C.F.R. Parts 160 and 162 and Part 164, Subparts A and C, the Security Standards for the Protection of Electronic Protected Health Information ("Security Rule"); Subtitle D of the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"), also known as Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, Public Law No. 111-005 ("ARRA"); and 45 CFR Parts 160 and 164 Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the HITECH Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule - all together, as amended from time to time, herein referred to as the "Privacy and Security Rules"; and

WHEREAS, Covered Entity and Business Associate acknowledge that each has obligations in its respective role as Covered Entity and Business Associate under the Privacy and Security Rules, as well as regulations promulgated thereunder; and

WHEREAS, Covered Entity and Business Associate intend to protect the privacy and provide for the security of PHI accessed by or disclosed to Business Associate pursuant to their Service Agreement in compliance with this BAA and the Privacy and Security Rules; and

WHEREAS, the purpose of this BAA is to satisfy certain standards and requirements of the Privacy and Security Rules, including the requirement of an appropriate agreement between Covered Entity and Business Associate that meets the applicable requirements of the Privacy and Security Rules.

NOW THEREFORE, in consideration of the mutual promises and covenants, herein, and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the parties agree as follows:

1. **Definitions.**

   Capitalized terms used in this BAA and not otherwise defined herein shall have the same meanings set forth in the Privacy and Security Rules which definitions are incorporated in this BAA by this reference.

2. **Permitted Uses and Disclosures by Business Associate.**

   a. *Performance of Services.* Except as otherwise limited in this BAA, Business Associate may only use or disclose PHI to perform the services set forth in the Service Agreement, as permitted or required by this BAA, or as Required by Law. Business Associate agrees to limit its uses, disclosures and requests for PHI to the minimum amount necessary to perform its obligations.

   b. *Proper Management and Administration*. Except as otherwise limited in this BAA, Business Associate may use or disclose PHI as necessary for Business Associate's proper management and administration or to fulfill its legal responsibilities, provided that: (1) the disclosures are Required by Law, or (2) Business Associate obtains reasonable assurances from the third party to whom the PHI is disclosed in the form of a written agreement with terms similar to and consistent with this BAA that the PHI will remain confidential and used or further disclosed only as Required by Law or for the purposes for which it was disclosed to the third party, and the third party notifies Business Associate of any instances of which it is aware in which the confidentiality of the PHI has been breached.

   c. *Data Aggregation.* Except as the parties might otherwise agree in writing, Business Associate shall only provide data aggregation services on Covered Entity's behalf if specifically directed to do so in writing.

   d. *De-Identified Information.* Business Associate may create, use and disclose de-identified information if required for purposes of providing Services. Business Associate shall not use Covered Entity's de-identified information for its own purposes, except on a case by case basis with Covered Entity's separate prior written agreement for a proposed use. De-identification must comply with 45 CFR §164.502(d), and any such de-identified information must meet the standard and implementation specifications for de-identification under 45 CFR §164.514(a) and (b), or as they may be amended from time to time.

3. **Prohibition on Certain Uses and Disclosures and Compliance with Transaction Standards.**

   a. *As Permitted in this BAA.* Business Associate shall not use or disclose Covered Entity's PHI other than as permitted or required by this BAA or as Required by Law. This BAA does not authorize the Business Associate to request, use, disclose, maintain or transmit PHI in any manner that violates the Privacy and Security Rules if done by Covered Entity.

   b. *Electronic Transactions*. Business Associate hereby represents and warrants that to the extent it is transmitting any HIPAA Transactions for Covered Entity, the format and structure of such transmissions shall be in compliance with the Transaction Standards provided that it is Covered Entity's responsibility to ensure that appropriate Code Sets are used in the coding of services and supplies. Business Associate shall indemnify and hold Covered Entity harmless from any monetary penalties assessed against Covered Entity arising from a breach of the representation and warranty contained herein, including reimbursing Covered Entity for any cost incurred by Covered Entity as a result of an audit or investigation by the Secretary which may include the costs of consultants and lawyers.

4. Compliance with the HITECH Act.

Business Associate shall comply with all additional requirements of the HITECH Act, including, but not limited to:

a. Compliance with the requirements regarding minimum necessary under HITECH § 13405(b);
b. Requests for restrictions on use or disclosure to health plans for payment or health care operations purposes when the provider has been paid out of pocket in full, consistent with HITECH § 13405(a);
c. The prohibition of the sale of PHI without authorization unless an exception exists under HITECH § 13405(d);
d. The prohibition on receiving remuneration for certain communications that fall within the exceptions to the definition of marketing under 45 C.F.R. § 164.501 unless permitted by this BAA and Section 13406 of HITECH;
e. The requirements relating to the provision of access to certain information in electronic format under HITECH § 13405(e);
f. Compliance with each of the Standards and Implementation Specifications of 45 C.F.R. §§ 164.308 (Administrative Safeguards), 164.310 (Physical Safeguards), 164.312 (Technical Safeguards) and 164.316 (Policies and Procedures and Documentation Requirements); and
g. The requirements regarding accounting of certain disclosures of PHI maintained in an Electronic Health Record under HITECH § 13405(c).

5. Safeguards, Subcontractors, Training and Enforcement.

a. *Safeguards*. In accordance with Subpart C of 45 CFR Part 164, Business Associate shall implement and use appropriate and industry best practice technical, procedural and physical safeguards to prevent unauthorized use or disclosure of Covered Entity's PHI, including implementing requirements of the Security Rules with regard to electronic PHI and all applicable laws, regulations and guidance documents. Likewise, Business Associate acknowledges that it is directly liable under the Security Rules and may be subject to civil and, in some cases, criminal penalties for:

   i. failing to safeguard PHI, including electronic PHI, in accordance with the HIPAA Security Rules; and

   ii. uses or disclosures of PHI that are not authorized by this BAA or Required by Law.

   Business Associate shall provide Covered Entity with information concerning the aforementioned safeguards and/or other information security practices as they pertain to the protection of Covered Entity's PHI, as Covered Entity may from time to time request.

b. *Agents/Subcontractors.* In accordance with 45 C.F.R. §§ 164.502(e)(1)(ii) and 164.308(b)(2), before disclosing any PHI received from Covered Entity or created on behalf of Covered Entity, Business Associate will enter into a written agreement with any agents and subcontractors that create, receive, maintain, or transmit PHI on behalf of Business Associate, and the terms of such agreement shall be at least as stringent as the restrictions and conditions with respect to the use, protection and disclosure of such PHI that that apply to Business Associate pursuant to this BAA. Business Associate will ensure that any agents and subcontractors to whom it provides PHI agree to implement reasonable and appropriate safeguards to protect such information.

c. *Training*. Business Associate shall provide all of its employees and members of its workforce who will have access to PHI with general HIPAA-related training and education prior to allowing the employees and members of its workforce access to PHI. Such training will be conducted at least annually.

d. *Audit, Inspection and Enforcement*. Business Associate agrees that upon reasonable notice of at least ten (10) business days, Covered Entity may audit the Business Associate's security and privacy policies and procedures, including its security safeguards, to ensure the appropriate protections are in place for Covered Entity's data. Such audit by Covered Entity may be performed by a third party of Covered Entity's choosing and expense to perform compliance analysis of Business Associate's practices with respect to the Privacy and Security Rules, including vulnerability or penetration testing or physical assessments of Business Associate's operations that relate to Covered Entity's PHI. The parties agree to cooperate so that such audits are coordinated to minimize any negative effect on the operation of Business Associate's database, application or systems as a result of such a review. Covered Entity will also provide Business Associate with a copy of the results of such testing. The fact that Covered Entity inspects, or fails to inspect, or has the right to audit or inspect Business Associate's facilities, systems, books, records, agreements, policies and procedures does not relieve Business Associate of its responsibilities to comply with the Service Agreement, this BAA, and applicable HIPAA Regulations, nor does Covered Entity's (i) failure to detect or (ii) failure to notify Business Associate of or to require Business Associate to remedy a detected unsatisfactory practice, constitute an acceptance of such practice by Covered Entity or a waiver of Covered Entity's enforcement rights under the Service Agreement or this BAA. In addition, Business Associate agrees to use good faith efforts to retain the right to audit the privacy and security policies and procedures of its agents and subcontractors who may use or disclose PHI.

e. *Service Organization Control Reports.* Due to the increased security, availability, processing integrity, confidentiality, and privacy risks of using Business Associate to deliver Services to or on behalf of Covered Entity, Business Associate agrees to annually provide a Service Organization Control 2 (SOC 2) Type 2 report to Covered Entity if (1) it provides Service Organization services to Covered Entity involving IU Health Confidential Information that Covered Entity would otherwise perform such as medical record services, data centers, IT managed services, software as a service (SaaS) vendors, and many other technology and cloud-computing based businesses, or (2) it is required as more particularly described in Exhibit A attached hereto. For the purposes of this BAA, IU Health Confidential Information shall mean all non-public information, including, but not limited to, PHI, limited data sets, payment information, personally identifiable information (PII), nonpublic personal information (NPI), Covered Entity proprietary information, sensitive data or information, such that unauthorized access to such data may result in serious financial, legal or operational impact to Covered Entity.

6. Obligation of Business Associate.

a. *Access to Information.* Within ten (10) business days of request from Covered Entity, Business Associate shall make available PHI in a Designated Record Set, to Covered

Entity, as necessary to satisfy Covered Entity's obligations under 45 CFR § 164.524, including providing or sending a copy to a designated third party and providing or sending a copy in electronic format, to the extent that the PHI in Business Associate's possession constitutes a Designated Record Set. Business Associate will not respond directly to an Individual's request for access to their PHI held in the Business Associate's Designated Record Set. Business Associate will direct the Individual to the Covered Entity so that Covered Entity can coordinate and prepare a timely response to the Individual.

b. *Amendment of PHI*. Within ten (10) business days of request from Covered Entity, Business Associate shall make any amendment(s) to PHI in a Designated Record Set, as necessary to satisfy Covered Entity's obligations under 45 CFR § 164.526. Business Associate will not respond directly to an Individual's request for an amendment of his PHI held in the Business Associate's Designated Record Set. Business Associate will direct the Individual to the Covered Entity so that Covered Entity can coordinate and prepare a timely response to the Individual.

c. *Accounting of Disclosures.* Business Associate agrees to document all disclosures of PHI which would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures in accordance with 45 CFR 164.528. Within ten (10) business days of notice by Covered Entity to Business Associate that Covered Entity has received a request for an accounting of disclosures of PHI, Business Associate shall make available to Covered Entity information to permit Covered Entity to respond to the request. Business Associate will not respond directly to an Individual's request for an accounting of disclosures. Business Associate will direct the Individual to the Covered Entity so that Covered Entity can coordinate and prepare a timely accounting for the Individual.

d. *Remuneration.* Business Associate shall not directly or indirectly receive remuneration in exchange for any PHI as prohibited by 45 CFR § 164.502(a)(5)(ii).

e. *U.S. Department of Health and Human Services*. Business Associate shall make available its internal practices, books, and records relating to the use and disclosure of PHI available to the Secretary of the Department of Health and Human Services for purposes of determining Covered Entity's compliance with the Privacy and Security Rules. Unless the Secretary directs otherwise or it is otherwise prohibited by law, Business Associate shall promptly notify Covered Entity of Business Associate's receipt of such request, so that Covered Entity can assist in compliance with that request.

f. *Judicial and Administrative Proceedings*. In the event Business Associate receives a subpoena, court or administrative order or other discovery request or official mandate for release of PHI, Business Associate shall notify Covered Entity in writing prior to responding to such request to enable Covered Entity to object. Business Associate shall notify Covered Entity of the request as soon as reasonably practicable, but in any event, within two (2) business days of receipt of such request.

g. *Reporting*. Business Associate shall immediately notify, no later than one (1) business day from discovery of a potential event affecting Covered Entity's data, the designated Chief Privacy Officer of the Covered Entity of: (1) any use or disclosure of PHI by

Business Associate not permitted by this BAA; (2) any Security Incident (*see explanation below)*; (3) any breach of unsecured Protected Health Information as defined in the HITECH Act; or (4) any other security breach of an electronic system, or the like, as such may be defined under applicable state law.

h. *Explanation of Security Incident.* For purposes of this BAA, "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. Covered Entity requires prompt notification from Business Associate if Business Associate experiences any Security Incident that compromises the confidentiality, integrity or availability of Covered Entity's data or information systems. Below are some examples of a Security Incident:

1) Business Associate information systems are exposed to malicious code, such as a virus or worm, and such code could be transmitted to Covered Entity's data or systems.

2) Unauthorized access is granted or obtained to servers or workstations that contain Covered Entity's data or Business Associate discovers that Covered Entity's data is being used, copied, or destroyed inappropriately.

3) Business Associate experiences an attack or the compromise of a server or workstation containing Covered Entity's information requiring that it be taken offline.

4) Unauthorized access, use or disclosure has occurred involving Protected Health Information, which is an obligation under the Privacy Rule.

The Parties agree that this section satisfies any notices necessary by Business Associate to Covered Entity of the ongoing existence and occurrence of attempted but Unsuccessful Security Incidents (as defined below) for which no additional notice to Covered Entity shall be required. For purposes of this BAA, "Unsuccessful Security Incidents" include activity such as pings and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above, so long as no such incident results in unauthorized access, use or disclosure of electronic PHI.

i. *Breach.* Within one (1) business day of discovery of a reportable Security Incident as described above or breach of unsecured PHI, Business Associate shall notify Covered Entity of the existence and nature of the incident as understood at that time. Business Associate shall immediately investigate the incident and within ten (10) business days of discovery shall provide to Covered Entity, in writing, a report describing the results of Business Associate's investigation, including:

1) the date of the breach;
2) the date of the discovery of the breach;
3) a description of the types of PHI that were involved;
4) identification of each individual whose PHI has been, or is reasonably believed to have been, accessed, acquired, or disclosed; and
5) any other details necessary to complete a risk assessment in accordance with the HITECH Act.

Reporting and other communications made to the Covered Entity under this section must be made to the Covered Entity's Chief Privacy Officer at:

Indiana University Health
ATTN: Privacy Counsel Office
340 W. 10th Street
Fairbanks Hall - Suite #3100
Indianapolis, IN 46202
Phone: 317-963-1940
Email: HIPAA@iuhealth.org

Business Associate shall cooperate with Covered Entity in investigating a breach and in meeting Covered Entity's obligations under the HITECH Act, and any other security breach notification laws or regulatory obligations.

Under certain circumstances, as solely directed by the Covered Entity, Business Associate will send or cause notifications to be sent directly to affected Individuals. Business Associate will comply with the requirements pursuant to 45 C.F.R. § 164.404. Prior to sending notification to the affected individuals, Business Associate will provide Covered Entity with an advance copy of the proposed letter for review and approval.

Business Associate shall be responsible for the mandatory reporting of breaches for which Business Associate is responsible to the Office of Civil Rights.

j. *Incident Costs.* In the event of a Breach of Unsecured PHI which Covered entity or other entity with Privacy and Security Rules enforcement jurisdiction determines was proximately caused by Business Associate for which HIPAA requires notice to be provided to individuals pursuant to 45 C.F.R. §§ 164.404 and 164.406, Business Associate shall be responsible for all costs associated with the incident, including but not limited to: (i) costs to print and mail the notification letters to affected individuals; (ii) media notification costs to the extent such media notification is required by applicable law; (iii) costs for Business Associate to set up a call center if Business Associate reasonably determines that such is necessary to handle inquiries; and (iv) credit monitoring costs if Covered Entity reasonably determines that it is necessary to mitigate harm for affected individuals.

k. *Mitigation*. Business Associate will cooperate with Covered Entity's efforts to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate not provided for in the Service Agreement or this BAA or that is not in accordance with HIPAA and the HITECH Act or other applicable law.

l. *Notice of Privacy Practices*. Business Associate will abide by the limitations of any Notice of Privacy Practices ("Notice") published by Covered Entity of which Covered Entity provides notice to Business Associate in accordance with the Covered Entity Obligations section of this BAA.

7. Obligations of Covered Entity.

a. *Notification of Changes Regarding Individual Permission*. Covered Entity will notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI. Covered Entity will provide such notice to Business Associate who shall implement the change no later than fifteen (15) business days after such notice. Covered Entity will obtain any consent or authorization that may be required by the Privacy or Security Rules, or applicable state law, prior to furnishing Business Associate with PHI. If the use or disclosure of PHI in this BAA is based upon an Individual's specific authorization for the use of his PHI, and the Individual revokes such authorization in writing, or the effective date of such authorization has expired, or authorization is found to be defective in any manner that renders it invalid, Business Associate agrees, upon receipt of notice from Covered Entity of such revocation or invalidity, to cease the use and disclosure of any such Individual's PHI except to the extent it has relied on such use or disclosure, or where an exception under the Privacy and Security Rules expressly applies.

b. *Notification of Restrictions to Use or Disclosure of PHI*. Covered Entity will notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522 or 42 U.S.C. § 17935(a), to the extent that such restriction may affect Business Associate's use or disclosure of PHI. If Business Associate reasonably believes that any restriction agreed to by Covered Entity pursuant to this Section may materially impair Business Associate's ability to perform its obligations under the Service Agreement or this BAA, the Parties will mutually agree upon any necessary modification of Business Associate's obligations under such agreements.

8. Insurance and Indemnification.

a. *Insurance*. Business Associate represents and warrants that during the term of the Service Agreement, it shall maintain commercially reasonable and sufficient insurance to adequately underwrite the potential risks associated with the Services, including but not limited to regulatory or administrative investigations or fines and appropriate cybersecurity coverage for privacy and security risks. This includes Business Associate's maintenance of cyber liability insurance with minimum limits of $5 million per occurrence. Upon request, Business Associate shall provide evidence of continuous coverage to Covered Entity and no coverage required within this section shall be voided or cancelled without prior notice to Covered Entity.

b. *Indemnification*. The Parties agree to indemnify, defend and hold harmless each other and each other's respective employees, directors, officers, subcontractors, agents or other members of its workforce, each of the foregoing hereinafter referred to as "indemnified party," against all actual and direct losses suffered by the indemnified party and all liability to third parties arising from or in connection with any breach by the indemnifying party or its employees, directors, officers, subcontractors, agents or other members of its workforce of this BAA or of any warranty hereunder or from any negligence or wrongful acts or omissions, including failure to perform its obligations under the Privacy and Security Rules. Accordingly, on demand, the indemnifying party shall reimburse the indemnified party for any and all actual and direct losses, liabilities, lost profits, fines, penalties, costs or expenses (including reasonable attorneys' fees) which may for any reason be imposed upon any indemnified party by reason of a suit, claim, action, proceeding, regulatory or administrative investigations or fines, or demand by any third party which results from the indemnifying party's breach hereunder. The Parties' obligation to indemnify any indemnified party shall survive the expiration or termination of this BAA.

9. Term and Termination.

a. *Term.* The term of this BAA shall be conterminous with that of the Service Agreement and shall terminate at the expiration or termination of that Agreement or when all of the PHI provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity.

b. *Termination for Breach.* Upon either party's knowledge of a material breach by the other party of this BAA, the non-breaching party will provide written notice to the breaching party detailing the nature of the breach and provide an opportunity for the beach to be cured within thirty (30) business days. Upon expiration of such thirty (30) day cure period, the non-breaching Party may terminate this BAA and, at its election, the Service Agreement, if cure has not been affected or is not possible.

c. *Effect of Termination.* Upon termination of the Service Agreement or this BAA, for any reason, Business Associate shall return or destroy (as directed by Covered Entity) all PHI received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, that Business Associate maintains in any form. Business Associate shall retain no copies of the PHI unless otherwise specifically agreed in writing by the parties. Business Associate shall certify in writing to Covered Entity the proper and timely return or destruction of PHI within ten (10) days of the termination of this BAA. If it is not feasible to return or destroy such PHI upon termination of this BAA, then Business Associate shall:

i. so inform Covered Entity, and Business Associate shall extend the protections of this BAA to the PHI and limit any further uses and disclosures;

ii. retain only that PHI which is necessary for Business Associate to continue its proper management and administration or to carry out Business Associates' legal responsibilities;

iii. continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic PHI to prevent use or disclosure of the PHI, other than as provided for in this Section, for as long as Business Associate retains the PHI;

iv. not use or disclose the PHI retained by Business Associate other than for the purposes for which such PHI was retained and subject to the same conditions set out above which applied prior to termination; and

v. when it becomes feasible, return to Covered Entity or destroy the PHI retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities. The terms and conditions of this section shall survive the expiration or termination of the Service Agreement.

For more information on the requirements for destruction of data, please see the Indiana University Health, Inc. Security Requirements in Exhibit A to this BAA.

10. Miscellaneous Provisions.

a. *Security Requirements*. Business Associate shall comply and shall cause its workforce to comply (to the extent applicable to individuals) with the provisions set forth in Exhibit A (referred to as the "Indiana University Health, Inc. Security Requirements"). As periodically requested by IU Health, but no more frequently than annually, Business Associate shall promptly, fully and accurately complete an IU Health Information Security Questionnaire and other documents or requests for information regarding Business Associate's information security practices.

b. *Continuity of Business*. Business Associate shall ensure that any and all data that it manages on Covered Entity's behalf shall be secured and backed up such that in the event that the Business Associate's services or data center containing Covered Entity's data suffers an adverse system event, Covered Entity shall be able to continue its business as intended with respect to the Services provided by Business Associate to Covered Entity under the Service Agreement. Therefore, Business Associate shall maintain such processes in place to ensure that in the event that it is bankrupt, data is corrupted or other interruption of its services that it has sufficient contingency plans in place to allow Covered Entity to continue its operations using the data it has entrusted to Business Associate.

c. *Notices*. Any notices pertaining to this BAA shall be given in writing and shall be deemed duly given to a Party or a Party's authorized representative identified in the Service Agreement in accordance with the Agreement's notice provision or, if no such provision exists, within three days of having sent the mail via certified USPS mail or via e-mail with electronic return-receipt received.

d. *Privacy and Security Responsible Individuals*. Business Associate shall provide to Covered Entity the contact information for primary individuals responsible for privacy and security compliance for Business Associate's organization. Business Associate agrees to update Covered Entity in the event that the primary responsibility falls to a different individual.

e. *Amendments*. This BAA and attached Exhibit A may not be changed or modified in any manner except by an instrument in writing signed by a duly authorized officer of each of the Parties hereto. The parties acknowledge that the Privacy and Security Rules and the HITECH Act may be modified from time to time. In the event of any such change, both parties agree to immediately enter into good faith negotiations to amend this BAA, through a written document signed by the parties, to conform to any new or revised legislation, rules and regulations to which the parties are subject.

f. *Interpretation*. Any ambiguity in this BAA shall be interpreted to permit the Covered Entity to comply with the Privacy and Security Rules and the HITECH Act.

g. *Geographic Limitations*. Business Associate shall not create, receive, maintain, transmit, use or disclose PHI outside of the United States without the written consent of Covered Entity.

h. *Choice of Law*. This BAA and the rights and the obligations of the Parties hereunder shall be governed by and construed under the laws of the State of Indiana, agreeing not to apply the conflict of laws principles.

i. *Assignment of Rights and Delegation of Duties*. This BAA is binding upon and inures to the benefit of the Parties hereto. Neither Party may assign any of its rights or delegate any of its obligations under this BAA without the prior written consent of the other Party, which consent shall not be unreasonably withheld or delayed.

j. *Data Ownership*. Unless otherwise specifically set forth in the Service Agreement, Covered Entity owns or controls, and shall continue to own or control, any and all data and PHI shared with Business Associate in order to allow Business Associate to perform its Services under the Service Agreement.

k. *Nature of BAA*. Nothing in this BAA shall be construed to create (i) a partnership, joint venture or other joint business relationship between the Parties or any of their affiliates, (ii) any fiduciary duty owed by one Party to another Party or any of its affiliates, or (iii) a relationship of employer and employee between the Parties.

l. *No Waiver*. Failure or delay on the part of either Party to exercise any right, power, privilege or remedy hereunder shall not constitute a waiver thereof. No provision of this BAA may be waived by either Party except by a writing signed by an authorized representative of the Party making the waiver.

m. *Severability*. The provisions of this BAA shall be severable, and if any provision of this BAA shall be held or declared to be illegal, invalid or unenforceable, the remainder of this BAA shall continue in full force and effect as though such illegal, invalid or unenforceable provision had not been contained herein.

n. *No Third Party Beneficiaries*. Nothing in this BAA shall be considered or construed as conferring any right or benefit on a person not party to this BAA or imposing any obligations on either Party hereto to persons not a party to this BAA.

o. *Headings*. The descriptive headings of the articles, sections, subsections, exhibits and schedules of this BAA are inserted for convenience only, do not constitute a part of this BAA and shall not affect in any way the meaning or interpretation of this BAA.

p. *Independent Contractors / No Agents*. Nothing contained in this BAA is intended to be, nor shall be deemed or construed to constitute Covered Entity and Business Associate as partners, joint ventures, co-principals, agents, or associates in connection with the Services and sharing of PHI, and Business Associate shall perform its duties and obligations hereunder as an independent contractor and not as an agent.

q. *Entire Agreement*. This BAA, together with any attached exhibits, statements of work, riders and amendments constitutes the entire agreement between the Parties hereto with respect to the subject matter hereof and supersedes all previous written or oral understandings, agreements, negotiations, commitments, and any other writing and communication by or between the Parties with respect to the subject matter hereof. In the event of any inconsistency between the provisions of this BAA and the provisions of the Service Agreement, the provisions of this BAA shall control as to the protection, use or disclosure of PHI. In the event of inconsistency between the provisions of this BAA and any mandatory provisions of the Privacy and Security Rules, as amended, or their interpretation by any court or regulatory agency with authority over Business Associate or Covered Entity, such interpretation or rule will control; provided, however, that if any relevant provision of or amendment to the Privacy and Security Rules changes the obligations of Business Associate or Covered Entity that are embodied in the terms of this BAA, then the Parties agree to operate in compliance with the amendment, interpretation or provision and to negotiate in good faith appropriate non-financial terms or amendments to this BAA to give effect to such revised obligations. Where provisions of this BAA are different from those mandated in the Privacy and Security Rules but are nonetheless permitted by such rules as interpreted by courts or agencies, the provisions of this BAA will control.

r. *Regulatory References*. A citation in this BAA to the Code of Federal Regulations or the Privacy and Security Rules shall mean the cited section or rule as it may be amended from time to time.

s. *Reciprocal Obligations*. In the event that Covered Entity acts as a "business associate" to Business Associate, then Covered Entity shall provide the same protections as Business Associate hereunder to Business Associate and agrees to be bound by the terms of this BAA the same as Business Associate with respect to such PHI of Business Associate.

IN WITNESS WHEREOF, the Parties have executed this BAA contemporaneously with the effective dates of the Service Agreement.

(Business Associate)	**(Covered Entity)**
Signed	Signed
Printed	Printed
Date	Date

All Business Associate Agreements must be reviewed and approved by the IU Health Privacy Office. Do not edit this document without permission of the Privacy Office or the Chief Privacy Officer. To contact the Privacy Office, please call 317-963-1940 or email HIPAA@iuhealth.org.

BUSINESS ASSOCIATE LISTING INFORMATION

In order to comply with the OCR request to provide detailed information about business associates, please provide the following information:

Type of Service(s) Provided: ____

Business Associate Privacy Officer
Name (printed): ____
Phone: ____
Address: ____
E-mail:____

Business Associate Security Officer
Name (printed): ____
Phone: ____
Address: ____
E-mail:____

Website URL: ____

Exhibit A

Indiana University Health, Inc. Security Requirements

These are minimum requirements required by IU Health's Information Security Program. We recognize that sound practices require continual assessment of evolving risks, technology and relevant issues related to information security. In the event that our Information Security Officer deems it necessary to modify these Security Requirements in order to continue to reasonably protect IU Health Confidential Information, then Business Associate will be notified and a remediation plan and timeframe will be mutually agreed upon. For the purposes of below, (i) each reference to "Agreement" shall be defined to include the BAA and Service Agreement, (ii) each reference to "Provider" shall be defined to include Business Associate, and (iii) each reference to "IU Health" shall be defined to include Covered Entity.

Any information technology system implemented as part of this Agreement that processes, stores, transmits, or receives information classified as Restricted or Critical by the IU Health Data Classification Policy is subject to the regulatory provisions regarding these data classifications, which include the Health Information Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standards (PCI-DSS), Family Educational Rights and Privacy Act (FERPA), and the HITECH Act. Therefore, any such system implemented as part of this Agreement must:

i. Demonstrate that it stores data at rest in compliance with the HIPAA Security Rule or PCI-DSS as applicable by either utilizing existing Provider's facilities (e.g., storage area network, file servers) to store data, or utilizes NIST FIPS 140-2 compliant encryption to store it local to the system itself.

ii. Demonstrate that it is able to securely transmit and receive PHI in compliance with the HIPAA Security Rule, HITECH Act, or PCI-DSS by utilizing NIST FIPS 140-2 compliant encryption.

iii. Demonstrate that data access requires a unique username/password or two-factor authentication (e.g., username and password, along with a personal identification number, certificate, software or hardware token, or smart card).

    1. Ideally, the system will demonstrate that users can be provisioned from already-existing directory systems utilizing either LDAP/S or Identity Management technologies such as Active Directory, OpenAthens, Shibboleth, or login.gov through Active Directory Federation Services or integration technologies.

iv. Provide the ability to log and monitor access to data

    1. Log the date, time, user id, requesting Internet Protocol (IP) address, subject ID(s), and actions taken by users to query, read, add, modify, or delete data about said subject(s).

    2. Provide the ability to query the logging and monitoring data by user, date, workstation or subject, or export said data in a structured format for reporting purposes.

    3. Provide the ability to export the data so that IU Health can retain it in accordance with the Center for Medicare and Medicaid Services' Office of Civil Rights (OCR) guidance on Cloud Computing, PCI-DSS, and internal IU Health policies on data retention.

        a. Ideally, the system would allow IU Health to receive the data over syslog or a similar protocol allowing it to be transmitted to the hosted Security Incident and Event Manager (SIEM).

v. Allow installation of IU Health supplied digital certificates and certificate chains to facilitate encryption utilizing Transport Layer Security (TLS) version 1.2 or greater technologies.

   1. If the system does not support TLS 1.2 or greater, please document the resolution and steps to update the system to handle it with an estimated completion date.

vi. Allow backup and recovery of digital certificates and encryption technologies utilizing existing Provider systems.

vii. Demonstrate overall systems compliance by providing the following for mandatory review by IU Health's Information Security Team:

   1. An overall system architecture diagram, which includes a demonstration of logical separation of client data that prevents commingling of data.
   2. A recommended network architecture implementation, including recommended segmentation, firewall rules, and network protection such as Data Loss Prevention to allow only applicable ports & protocols to protect data.
      a. In the case of PCI-DSS compliance, this is required.
   3. A documented example of an actual system implementation.
   4. If this is a cloud-based or hosted system, a documented network architecture showing the security controls in place (e.g., firewalls, IDS/IPS, authentication, Data Loss Prevention, etc.).
   5. Provider references for security implementations.
   6. Demonstrated backup and recovery procedures.
   7. Demonstrated user access management procedures.
   8. Static code analysis utilizing a verified third-party tool to ensure provided source code does not have any security issues.
   9. A risk assessment of the application environment, with a documented issues list and plan to address discovered issues on at least an annual basis.
   10. A risk management plan to continually address and remediate discovered issues.
   11. Periodic vulnerability testing of the environment to discover and remediate potential vulnerabilities.
   12. If the system is handling PCI-DSS data:
      a. A third-party penetration test performed by a certified PCI QSA on a quarterly basis.
      b. If systems and data are to be hosted in a non-Provider location, please provide the following for any facility or third party which will be storing, hosting, or processing said systems or data:
         i. A Service Organization Controls 1 (SOC 1) Type 2 Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting.
         ii. A Service Organization Controls 2 (SOC 2) Type 2 Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy.

We require that both reports be completed to standards set by the American Institute of Certified Public Accountants (AICPA), and be completed by a licensed CPA firm.

13. A Data Destruction Policy which demonstrates that data no longer in use or required to be retained will be destroyed to National Association for Information Destruction (NAID – www.naidonline.org) standards.

viii. Provide support for the application(s) running on a defined set of:

1. Operating Systems and supporting system services (e.g., OpenSSH, OpenSSL, Apache, Systemd).
2. Relational Database Management System Software (e.g., Oracle, SQL Server, MySQL).
3. Third-party software such as Application Servers, Web Servers, Security Software, Support Libraries, and other software required for daily operation of the application(s)

ix. If there are discovered security vulnerabilities in the previously described items and/or the application(s), the following need to be provided within 48 hours to IU Health:

1. Mitigation steps that IU Health can undertake to mitigate the reported vulnerabilities.
2. A timeline for any application patches that need to be applied to the environment to mitigate vulnerabilities.
3. A timeline for testing and approval of patches to any of the supporting items described above.

x. If there are discovered security vulnerabilities in the previously described items and/or the application(s), the following need to be provided within seven (7) days to IU Health:

1. Instructions for patching the supported items to restore the security posture of the environment.
2. Instructions for patching the application to restore the security posture of the environment.

xi. Ensure that the Operating System, any Relational Database Management System Software, and Third-Party software is supported by both the system and/or software vendors for the system lifecycle with system updates and security patches. If any of these components become unsupported, the Provider needs to address this before the system has an unsupported component.

xii. Provide documentation on the organization's Incident Response Plan, and a current list of security contacts for reporting vulnerabilities or compliance issues.

xiii. Allow IU Health the right to audit information systems in the scope of the system(s) in scope of this Agreement.

xiv. Provide IU Health responses to the provided Vendor Risk Assessment and Security Questionnaire. Any misrepresentation on either of these documents may result in contract termination.

xv. Provide IU Health a data dictionary and instructions on how to extract data in a defined industry-standard format (e.g., Text, database backup, etc.) using industry standard methods that will allow retrieval and analysis to meet data retention guidelines as specified by federal and state law, and guidance issued by the Office of Civil Rights.

Lasalle University

Implementing Secure Cloud Computing in the Small to Medium-Sized Healthcare Environment

May 2012

LASALLE UNIVERSITY

Implementing Secure Cloud Computing in the Small to Medium-Sized Healthcare Environment

INL 880 Capstone Project

Mitch Parker and Javier Aguero

5/4/2012

Abstract: There is a growing push to have small to medium-sized healthcare providers adopt Electronic Health Record or Electronic Medical Records systems as part of Federal incentive programs. The costs of these systems are causing vendors to look at cloud-based systems to host their data. We look at the potential risks and devise system selection, mitigation, and implementation strategies to provide organizations with the ability to secure their data both locally and in the cloud.

Contents

Executive Summary

There is a growing trend to have small to medium-sized healthcare providers adopt certified Electronic Health Records (EHR) or Electronic Medical Records (EMR) systems as part of Federal Meaningful Use incentive programs to modernize the delivery of healthcare. The major barrier to adoption of these systems is the implementation cost. There are multiple providers of outsourced and cloud-based certified EMR or EHR systems who promise to provide security that meets the required standards, which are defined in the Health Information Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH), and the Meaningful Use financial incentive programs from the Center for Medicare and Medicaid Services. These solutions can provide healthcare practitioners with significant cost savings over hosting their own EMR system.

The addition of an EMR system to a medical practice adds significant risk and the potential for financial and reputational damage because an unauthorized data breach is equally great. The addition of any EMR system to any medical practice requires additional security and processes. The implementation of a cloud-based or outsourced solution does not immediately provide the security an organization needs to protect them. There are multiple other factors which affect the security of any medical office or EMR system that need to be addressed.

This provides a comprehensive solution set to address these issues and mitigate risks. This involves the development of a selection instrument based on federal regulations which can be used by small to medium-sized healthcare providers to determine if their choice of cloud-based EMR systems meets the requirements as

stipulated under HIPAA, HITECH, and Meaningful Use. To address residual risk in the offices identified during the creation of the instrument, a vendor selection process based on the criteria in the instrument is used to find solutions to those issues. A recommended implementation strategy for a small to medium-sized healthcare provider is then provided. The benefits and lessons learned are then discussed along with salient points for the overall conclusion.

Introduction

Over the past few years, there have been multiple advances in technology and networking that have put the reach of large-scale networked systems within the hands of everybody, especially healthcare providers. Since 1985, when the Veterans Administration installed the first comprehensive Electronic Health Record, VistA, in all of its clinics (WorldVista Inc., 2012), there has been a push to utilize electronic medical records systems to store patient data and make it easily accessible to both providers and patients.

There has also been another push from within the medical field itself to use technology to provide better patient care. Many medical professionals, not just doctors, have availed themselves of the latest technologies to support their practices. Some of these technologies include smartphones, tablet computers, interactive web applications, and electronic medical records systems. Some of these allow for full access to patient charts and medical records. One of the largest vendors of Electronic Medical Records, Epic, offers an application for this called Haiku which runs on the iPhone (Epic Systems, 2012).

Recently, there have been three major pieces of legislation that have caused small to medium-sized medical practices to want to adopt Electronic Medical Records (EMR) or Electronic Health Records (EHR) systems. The first piece is the Health Information Portability and Accountability Act, known as HIPAA, which enforces stringent privacy and security rules, as well as standardized code sets for reporting transactions (CMS, 2012). HIPAA is a very important piece of legislation because it provides for patient privacy, through access to medical records by the patient and their designated appointees, and legal enforcement of the patient's privacy through specific violations (CMS, 2012). HIPAA is the major driver behind many of the practices in healthcare organizations today, because it mandates standardized code sets and reports along with privacy and security standards which EMR or EHR systems must follow.

The second piece is the amendment to HIPAA that is part of the American Recovery and Reinvestment Act of 2009, known as ARRA or the Stimulus Act (recovery.gov, 2012). ARRA includes a provision known as the Title XIII - Health Information Technology for Economic and Clinical Health Act and also known as the HITECH Act (GPO, 2009). The HITECH Act provides for stiffer penalties for organizations that violated HIPAA, up to $1.5 million per violation (GPO, 2009). It also requires organizations to be more proactive about weaving security into their mainstream activities (Long, 2011). And it also provides financial incentives for many types of medical providers, from small medical offices to large academic hospitals, to adopt Electronic Health Record or Electronic Medical Record technologies (GPO, 2009). These funds are dispersed when the organization demonstrates that the electronic health record systems are used and meet certain criteria.

The criteria for government financial incentives related to EMR are defined as part of the Center for Medicare and Medicaid Services' (CMS) Meaningful Use Incentive Programs (CMS, 2012). This is the third piece of legislation campaigning for Electronic Health Records (EHR). These three criteria, which were originally defined as part of the HITECH Act, include using an EHR in a certified manner, such as e-prescribing; using a certified EHR for electronic exchange of health information to improve quality of health care; and using certified EHR technology to submit clinical quality and other measures (CMS, 2012). Stage 1 of the incentive programs began in 2011, and Stages 2 and 3 will (tentatively) be implemented in 2013 and 2015, respectively (CMS, 2012). These programs are designed to advance medical practices toward full adoption of EMR/EHR systems.

These requirements and financial incentives signify a multifaceted problem. There are a large amount of smaller medical practices and healthcare organizations that would not be able to implement Electronic Health Records without the use of federal incentive dollars because of the high cost of implementation (Kumar and Aldrich, 2010). HIPAA Compliance is expensive, and is also often times confusing. A small industry of Electronic Health Record providers has emerged over the past several years offering certified systems for smaller providers. These systems are hosted in the cloud or remotely at other sites. The reason why remote hosting is implemented is because many medical practices cannot afford to host their own systems, or hire their own IT staff to maintain them (Valdes, Kibbe, Tolleson, Kunik, Petersen, 2004).

Therefore, smaller organizations consider implementing a lower-cost model, such as an Application Service Provider or Cloud Computing solution for their Electronic

Medical Records system. The cost savings of a cloud computing model as opposed to in-house can be anywhere from 50% to 90% of the final system cost (Mell and Grance, 2009). Cooper University Hospital realized significant implementation cost savings by outsourcing their Epic implementation to ACS. Michael Sinno, former CIO of Cooper University Hospital indicated that he was able to save costs and implement Epic for $18 million as opposed to the implementation costs for an in-house solution. In addition, there are other costs to consider in terms of system maintenance.

Cloud Computing is one of the latest buzzwords in IT computing, with multiple first-tier providers such as Amazon, Rackspace, and Intuit offering Software as a Service (SaaS) to customers. They offer systems where the customer pays for everything as a service in one bill, as opposed to multiple services or applications (Armbrust, 2010).

Most importantly, information loss or misuse because of a data or security breach becomes the problem of the provider (Nahra, 2008). The reputation of the providers themselves is compromised (Long, 2011). Therefore, there is a need for additional security and security processes in a small to medium sized provider environment, because putting an Electronic Health Record or Electronic Medical Record system in place adds a degree of risk that was not there before, especially if the solution is outsourced to one of the providers.

Organizations using outsourced solutions need to answer specific questions. First are these solutions really compliant when looked at in the context of their implementation in a medical office setting? Second, is a “cloud” solution secured, and can the risks be identified and mitigated? Third, what security is needed for computers in the offices or with devices that access the system? The chief issue with an EMR or EHR cloud solution issue is that the implementation of a certified EHR system is only one component of Meaningful Use. A cloud-based solution, which may help an organization receive incentive money from the US Government, may not have the security that an organization needs to adequately protect its data. This is because the use of a certified system does not guarantee that the systems which access it are also secure.

This paper provides a framework for small and medium-sized healthcare organizations to effectively implement a cloud-based Electronic Health Record solution that will protect their patients, their organizations, and their employees. It focuses on technology strategies needed and provides a model to effectively implement the managerial and technical controls.

EMR Technologies and the Current Situation with Meaningful Use Certification

Currently, the most prevalent technology used in the healthcare environment is the Electronic Health Record (EHR) or Electronic Medical Record (EMR). The definition from the Department of Health and Human Services (HHS) is:

> An EMR (electronic medical record) is a real-time patient health record with access to evidence-based decision support tools that can be used to aid clinicians in decision-making. The EMR can automate and streamline a clinician's workflow, ensuring that all clinical information is communicated. It can also prevent delays in response that result in gaps in care. The EMR can also support the collection of data for uses other than clinical care, such as billing, quality management,

outcome reporting, and public health disease surveillance and reporting (HHS, 2012).

EMR systems can contain multiple modules, including Emergency Medicine, Laboratory Medicine, Radiology, Operating Room, Ambulatory Care, and Acute Care (Epic Systems, 2012). They are used to organize all of the information on a patient in one place, and can facilitate access by outside agencies or the patients themselves (Epic Systems, 2012).

Currently, the United States government provides financial incentives for adoption of EMR systems by practices and hospitals. This program, Meaningful Use, has been in place since 2010 (Medicare and Medicaid Programs; Electronic Health Record Incentive Program; Final Rule, 2010). Meaningful Use, which was originally part of the HITECH Act (Section 4101c), provides incentive payments to providers who adopt EMR technology. It also provides for financial penalties for organizations who do not adopt this technology by 2015 (Medicare and Medicaid Programs; Electronic Health Record Incentive Program; Final Rule, 2010). The penalties will be lower payment rates for organizations that do not adopt EMR or EHR systems.

The Certification Commission for Health Information Technology (CCHIT) is authorized by the Department of Health and Human Services to offer certification services under the guidance of the Office of the National Coordinator – Authorized Testing and Certification Body (ONC-ATCB) of the Department of Health and Human Services (HHS) (CCHIT, 2012). Only organizations that implement EMR systems which are certified by CCHIT with ONC-ATCB certification are eligible to continue to apply for incentive payments (CCHIT, 2012) (Medicare and Medicaid Programs; Electronic Health Record Incentive Program; Final Rule, 2010).

There are three categories of certification by CCHIT. The first is ONC-ATCB, which is the most rigorous, and ensures that the EMR that the organization is implementing meets the certification criteria established by the Secretary of the Department of Health and Human Services (CCHIT, 2012). The second is CCHIT Certified, which includes a rigorous inspection of integrated EHR functionality, interoperability, and security according to criteria independently developed by the CCHIT's multi-stakeholder and expert work groups using CCHIT's published testing methods (CCHIT, 2012). This does not necessarily include the certification criteria from the Department of Health and Human Services. Finally, there is the EHR Alternative Certification for Healthcare Providers, or EACH (CCHIT, 2012). This allows organizations that have developed their own EMR/EHR system to certify their system with CCHIT with the ultimate goal of attaining ONC-ATCB certification so that they qualify for financial incentives (CCHIT, 2012).

There are multiple issues with the implementation of EMR systems by healthcare providers. The first is the cost, which is the biggest barrier (Zhivan and Diana, 2012). EMR systems can cost over $100 million to implement for a large healthcare system, such as the Epic implementation undergone by Geisinger Health System. This system costs 4.6% of their $2 billion annual revenue to maintain (Geisinger, 2012). EMR systems can also fail if the organization does not adopt it as an overall strategy with support from top leadership and support from all stakeholders. An example is the failed $34 million dollar EMR initiative at Cedars-Sinai Hospital (Kumar and Aldrich, 2010). Additionally, there is the perception that the implementation may make the hospital or provider more inefficient (Zhivan and Diana, 2012).

Requirements Mapping and Development of a Security Evaluation Instrument

To properly define the requirements for an EMR/EHR system in a format that may be used to provide small and medium-sized businesses, a tool can be used as part of the systems selection process. The requirements for these systems need to be distilled down to a matrix which will cover all of the requirements, and whether they are the responsibility of the vendor/cloud services provider, health care organization, or both. T

The matrix instrument (found in appendix A) will provide organizations who are seeking to implement cloud-based or hosted Electronic Medical Records solutions with a checklist of controls to follow before a successful implementation of a system is hosted remotely or in the cloud. Following these controls will help an organization meet the requirements of the HIPAA Security Rule, Breach Notification Rule, ONC-ATCB, HITECH regulations, Healthcare Information Technology Standards Panel (HITSP) controls, and American Institute of Certified Public Accountants (AICPA) Service Operational Controls reporting requirements. The regulations do not make certain issues, such as the proliferation of removable storage and its impact on the HIPAA Security Rule, obvious. The requirement for encryption of data at remote sites is needed so that only authorized users can access protected health information in accordance with ONC-ATCB certification criteria.

The matrix lists the requirements from the HIPAA Security Rule, and then maps the Breach Notification Rule and HITECH Regulations on top of them. The ONC-ATCB certification requirements are also mapped. The HITSP controls are put on top of these to provide further assertions that these controls met both federal laws and industry standards. An AICPA control for Service Level Agreements was added so that organizations have the ability to have a contract in place that defines and measures service levels as the first requirement (AICPA, 2011). Finally, the Service Organization Controls SOC 2 reports requirements for remotely hosted data services were added. The purpose of SOC 2 reports is to measure the effectiveness of the relevant controls that an organization implements to protect the privacy and security of a system. If the hosting organization cannot meet SOC 2 requirements, it means that it does not have effective policies and procedures in place for protecting data as per the HIPAA Security Rule. The SAS 70 report will no longer work (AICPA, 2011).

The matrix is broken down into six major categories to address the issues. The first category is Encryption, which addresses the requirements for encryption of data at rest and in transit. The second category is Technical Policy and Unique User Identification/Access Control, which covers the technical implementation of a multi-user system that handles Protected Health Information (PHI). The third category is Proxy Server/Data Loss Prevention. This addresses potential breaches caused by improper data transmission. The fourth category is Firewall, which addresses the protection of the network from unauthorized access. Fifth is Antivirus, covering the protection of PCs and devices from malicious software. Sixth and final is Policies, Procedures, Risk/Impact Analysis, and Contracts, which cover the non-technical aspects of system implementation, specifically with organizational policies and procedures, system certification, business associate agreements, and risk/business impact analysis.

The matrix provides clarity throughout the system implementation process. While there are many sets of rules, this tool provides a comprehensive guide that can be used as a checklist to protect their organization by making sure that the solution is the right choice for compliance with the rules in the first place.

Developing Secure Solutions

One of the major issues with examining the myriad of regulations is having a small or medium-sized business effectively implement them. While a cloud-based solution may be able to provide security on the services side, the overall risk mitigation for the organization is not totally addressed. Kurt Long, in his article “Proactive Defense”, from the July 2011 issue of Hospital and Health Networks, indicates that organizations need to implement the following Information security and Privacy technologies to become compliant:

1. Employ a reputable, specialized third party to perform a gap analysis of information security and provide a report for the board.
2. Implement technologies and associated policies for encryption of all portable devices.
3. Initiate breach monitoring and protection for all systems that access protected health information.
4. Automate detection of privacy breaches related to identity and medical identity theft and unauthorized employee access to celebrities, friends, family and neighbors' records.
5. Automate privacy audit reporting across all applications that access protected health information.
6. Ensure electronic health record and other application vendors produce audit trails.
7. Create a chief information security officer position empowered with the appropriate authority and resources to identify and mitigate privacy breaches (Long, 2011).

The selection matrix developed in the previous section not only addresses these issues, it also addresses several gaps that Long did not address, specifically encryption of data at rest, authentication of unique users to the EMR system, secure configuration of endpoints, and network security. The matrix will be used to develop the criteria to evaluate the secure solution set.

Many small to medium-sized businesses still use consumer-level technologies such as Linksys routers or consumer-level PCs from stores such as Best Buy to run their businesses. The biggest risks for any solution that implements e-commerce, Cloud, or ASP technologies are the endpoints and server systems (Marchany and Tront, 2002).

One of the major reasons the Cloud is so attractive is because anyone can buy a computer and run the software from anywhere that has an Internet connection (Hawthorn, 2009). Today, especially with the number of persistent threats on the Internet, this is very risky behavior (Hawthorn, 2009).   The current technology needed for checking a machine's health every time it logs into a web site, Network Access Control (NAC), requires a significant amount of hardware and software engineering, and requires significant organizational coordination (Snyder, 2012). Many small to medium-sized businesses, and even some of the larger-sized ones, just don't have the resources to implement this. In addition, a solution that keeps a customer from accessing what they need for business may cause more issues than it solves, and it may be career-ending for the IT consultant who implements it (Snyder, 2012).

The technical and policy solution proposal set is something that an organization can implement for a lower cost using a combination of Free or Open Source and commercial software to implement the suggestions in Long's article.   Valdes, Kibbe, Tolleson, Kunik, and Petersen, in their article "Barriers to Proliferation of Medical Records", directly cite the use of Free and Open Source software as a way to help increase the adoption of EMR systems with practices (Valdes, Kibbe, Tolleson, Kunik, Petersen, 2004). The strategy is a best of breed environment with a combination of Free and Open Source software combined with commercial software that meets the customers' needs.

Many small and medium-sized businesses cannot afford the managed security services provided by companies such as Dell, Symantec, IBM, Verizon, or TrustWave. However, many of them already have local consultants that help with their systems. These consultants can implement these systems and recommendations, and the instructions are already available on the Internet. If there is skilled help needed, there are multiple consulting companies that are able to help with implementing these solutions.

The use of the recommendations for network security will provide small to medium-sized organizations with the ability to meet HIPAA, HITECH, and ONC-ATCB regulations by using a lower-cost solution to replicate the same results as much more expensive solutions that larger businesses implement, with an emphasis on compliance that is enough to meet requirements without compromising security.

To solve for these issues, the Cloud-based/Remotely Hosted Security Evaluation Matrix will develop a set of technical and policy requirements. The options for each requirement will be examined, including advantages, disadvantages, and costs. After this is done, a final solution set will be chosen and then summarized.

To satisfy the technical controls, a protection profile needs to be developed. The operating system for the client workstations is assumed to be Microsoft Windows. Three of the major EMR software packages, which are Siemens Soarian, Cerner Millenium, and Allscripts, require Windows clients (Siemens, 2012) (Cerner, 2012), (Allscripts, 2012). In addition, Microsoft Windows had 88.69% of the operating system share for the time period of May 2011 to March 2012 based on the NetMarketShare statistics, which were based on the usage logs of 12,049 service providers (NetMarketShare, 2012). Therefore, it is statistically very likely that an organization will be running Microsoft Windows. Customers should run Windows 7 Professional, Enterprise, or Ultimate Edition, as they can be joined to an Active Directory realm to enforce security policies (Microsoft, 2012). It can be purchased as either a standalone OS, as an upgrade from Windows 7 Home Premium or Starter Edition, or with a new PC from a manufacturer such as Dell (Microsoft Store, 2012).

Table 1: Microsoft Windows 7 Client Features

	Microsoft Windows
Market Share for May 2011-March 2012 time period	88.69%
Support from major EMR systems	Siemens, Cerner, Allscripts
Recommended Version	Windows 7 Professional, Enterprise or Ultimate

For server software, customers should run Windows Server Small Business Server 2011 or Server 2008 R2 as a small office server. The Windows Server platform, as of Q3/Q4 2009, according to International Data Corporation, had 73.9% of the server operating system market (Foley, 2010). It also comes with Active Directory, which allows for the effective management of users, computers, printers, groups, applications, and other directory-enabled objects from one central location (Microsoft, 2012). Windows Small Business Server 2011 also comes with Microsoft Exchange Server 2010 for e-mail, and supports BitLocker for server disk encryption, Windows Software Update Services, and SharePoint Foundation 2010 for collaboration (Microsoft, 2011)

(Techotopia.com, 2012). It is reasonably priced, with Dell supporting configurations that cost as little as $1,197.00 (Dell.com, 2012). Additionally, technologies such as Microsoft SQL Server, which is required by several management platforms, can run on Windows Server (Microsoft, 2012).

Table 2: Features of Windows Server

	Windows Server
Market Share as of Q3/Q4 2009	73.9%
Centralized management of users, computers, groups, printers, and applications	Active Directory
Built-in Encryption support	BitLocker
Software Updates	Windows Software Update Services
Collaboration Support	SharePoint Foundation 2010
E-mail Support	Exchange Server 2010
System Cost	$1197.00

There are six different protection categories from the matrix under the protection profile required for a small to medium-sized provider to have the correct technical controls in place to satisfy the technical protection profile. The categories are summarized below:

Table 3: Protection Categories

Category	Description
Encryption	Protects data on USB and removable disks, PCs, and servers by using encryption to protect the contents
Technical Policy/Unique User Identification and Access Control	Configures PCs to meet a minimum set of security criteria by implementation and enforcement of configuration controls, and provides for the authentication and identification of users in a multi-user environment.
Proxy Server and Data Loss Prevention	Prevents unauthorized breaches by monitoring client endpoint activity, sending data for further analysis to a Data Loss Prevention Server, and preventing unauthorized data transfers.
Firewall	An appliance that mediates access to the network given a set of rules on what connections to allow or deny.
Antivirus	Protects PCs against known or potential malware and threats.
Policies and Procedures	Provide the management frameworks to ensure accurate implementation of the EMR system.

These are the categories from the matrix which need to be satisfied to ensure that a provider meets the technical and policy requirements under the HIPAA Security Rule, HITECH Act, Breach Notification Rule, and ONC-ATCB requirements.

Encryption

For encryption, there are two different types of encryption to consider which are USB/Removable Disk and data at rest. Section A of the matrix, Encryption, addresses the requirements for encryption for both types. Since there are different product requirements for both types, they are evaluated as separate categories.

For USB/Removable Disk encryption, four products were considered. Each of these products is widely used already to protect data. The first option was TrueCrypt, which is an Open Source disk encryption platform which works on fixed disks and removable media (TrueCrypt, 2012). Next was McAfee’s Encrypted USB Platform, which uses a combination of McAfee USB Flash Drives and management software to manage encrypted removable media (McAfee, 2012). Third was Symantec Endpoint Encryption Removable Storage Edition, which allows usage of any USB drives with its management software to effectively manage removable media (Symantec, 2012). Fourth and final was Microsoft BitLocker To Go, which is built into the Windows 7 Ultimate and Enterprise Editions (Microsoft, 2012).

TrueCrypt is the only disk encryption system that will work on every major platform, including Windows, Linux, and Mac OS X (TrueCrypt, 2012). It is also free (TrueCrypt, 2012). However, the USB drive encryption is manual, and it does not provide automatic key management. This makes compliance with control A100, Emergency Controls; very difficult in that it would require a process step to store recovery keys for each piece of media encrypted (TrueCrypt, 2012). This would be onerous in a smaller office. It is also not FIPS 140-2 compliant, which causes control A105 to fail (TrueCrypt, 2012). Finally, it also does not have robust audit logging or tracking of drive usage, which causes control A103 to fail (TrueCrypt, 2012).

McAfee's FIPS 140-2 compliant platform requires special McAfee USB drives, and will work on Windows XP, Vista, and Windows 7 (McAfee, 2012). A 4 GB McAfee USB drive is $89.99 from CDW.com, with a minimum of 10 required to purchase (CDW.com, 2012). In comparison, a 4GB Lexar flash drive from newegg.com is $5.99 (Newegg.com, 2012). For management, logging, and emergency controls, ePolicy Orchestrator 4.0 (which requires Active Directory) and the license manager are also required (McAfee, 2012). These also have recurring licensing costs (CDW.com, 2012). McAfee ePolicy Orchestrator also requires software that needs to be run on Windows Server (McAfee, 2012). McAfee ePolicy Orchestrator costs $18.99 per user, plus

$2.462.00 for SQL Server 2008 R2 (CDW.com, 2012). A major disadvantage is the $89.99 cost per USB drive that can only be used with the system. However, it does meet all of the required controls.

Symantec's solution has extensive support for all USB flash drives, external hard disks, and even CD/DVD drives (Symantec, 2012). It is also able to integrate with the Symantec DLP solution (Symantec, 2012). It provides automatic key management and recovery (Symantec, 2012). In addition, it is also FIPS 140-2 compliant and can create self-extracting encrypted file archives, which support different distribution models (Symantec, 2012). It also requires a management server and Active Directory in the client environment to comply with control A100, Emergency Controls (Symantec, 2012). This solution costs approximately $50 per user per year to implement (CDW.com, 2012). It also complies with all of the required controls.

Microsoft's solution requires Windows 7 Ultimate or Enterprise Edition (Microsoft, 2012). It provides automatic key management and recovery with Active Directory (Burchill, 2010). It is also FIPS 140-2 compliant (NIST.gov, 2012). It can be configured extensively through Active Directory (Burchill, 2010). It does not provide the logging or auditing of USB drive usage that the McAfee or Symantec solutions provide, which causes control A103, Device and Media Controls, to fail (Beaver, 2009). There are also additional upgrade costs for implementing Windows 7 Ultimate or Enterprise. The cost to upgrade is $129.95 for Professional, $139.95 for Home Premium, and $169.95 for Starter Edition (Microsoft Store, 2012).

Based upon the requirements, the only recommended solution that meets all four requirements at a reasonable cost is Symantec Endpoint Edition Removable Storage

Edition. This solution uses any USB drive, and even supports burning CD-ROM disks (Symantec, 2012). It also allows for robust audit logging, key recovery from a management console, and FIPS 140-2 compliant encryption. While McAfee does have a solution that also meets all of the requirements, they require the usage of their flash drives, which is costly. BitLocker does not provide the logging or auditing required to prove that flash drives are encrypted. TrueCrypt is not certified, does not provide logging or auditing requirements, and is very difficult to manage as recovery keys have to be generated for each piece of encrypted media (TrueCrypt, 2012).

Table 4: Removable Storage Encryption Comparison Matrix

	TrueCrypt	**McAfee Encrypted USB**	**Symantec Endpoint Encryption**	**Microsoft BitLocker To Go**
Cost	$0.00	$89.99 per drive + $18.99/user for ePolicy Orchestrator license + $2462.00 for SQL Server	$50 per year	$129.95-$169.95
FIPS 140-2 Compliance	No	Yes	Yes	Yes
Key Management/ Emergency Access	Manual	Automatic	Automatic	Automatic
Logging	No	Yes	Yes	Does not provide proof of encryption
Requires special USB media?	No	Yes	No	No
Encrypts CD-ROM disks?	No	No	Yes	No
Recommended Solution	No	No	Yes	No

For Encryption of Data at Rest, four options were examined. Each of these solutions is already used to protect data in client environments. The first solution for encryption of data at rest that was examined was Symantec's PGP Whole Disk Encryption. McAfee Endpoint Encryption is evaluated for at rest, TrueCrypt was examined, and Microsoft BitLocker.

Symantec's PGP Whole Disk Encryption solution allows the entire hard disk of a target system to be encrypted (Symantec, 2012). It supports Windows 2000 through Windows 7 on the desktop, and Windows Server 2003 to 2008 R2 on the server side (Symantec, 2012). It also supports Linux and Mac OS X (Symantec, 2012). It requires an additional server component, PGP Universal Server, to manage it and bring it into compliance with control A111b, and Emergency Access by supporting emergency access and key recovery (Symantec, 2012). It is also certified for compliance with FIPS 140-2 and Common Criteria, satisfying control A105 – Encryption (Symantec, 2012). It also has extensive compliance reporting options (Symantec, 2012). The cost, however, for one machine per year is $154.00 for Essential Support (Symantec, 2012).

McAfee's Endpoint Encryption solution also allows the encryption of entire hard disks (McAfee, 2012). It supports Windows XP through Windows 7 on the desktop, and Windows Server 2003 to 2008 on the server side (McAfee, 2012). It supports Mac OS X and requires ePolicy Orchestrator to provide the management, emergency access, and key management components (McAfee, 2012). ePolicy Orchestrator also provides reporting, auditing, and proof of protection in reporting (McAfee, 2012). It is FIPS 140-2 compliant (McAfee, 2012). The cost of the license for McAfee Endpoint Encryption is $85.99 per license with one year of support (CDW.com, 2012).

TrueCrypt also supports the encryption of entire hard disks using multiple methods, including passphrases and key files (TrueCrypt, 2012). It supports Windows 2000 through Windows 7 on the desktop, and Windows Server 2000 to 2008 R2 on the server side (TrueCrypt, 2012). It supports Linux and Mac OS X (TrueCrypt, 2012). However, it requires manual management of key files and recovery disks for each PC to support recovery of and access to encrypted data (TrueCrypt, 2012). This can be very daunting for a small medical office. It is not FIPS 140-2 compliant, which causes control A105 – Encryption to fail (TrueCrypt, 2012). Due to its decentralized nature, TrueCrypt does not provide centralized management and proof of encryption, which causes control A103 – integrity to fail (TrueCrypt, 2012).

Microsoft BitLocker supports the encryption of fixed disks using passphrases, Active Directory credentials, or smart cards (Microsoft, 2012). It supports Windows 7 Enterprise or Ultimate editions only on the desktop, and Windows Server 2008 and 2008 R2 on the server side, which can limit its effectiveness (Microsoft, 2012). It is also FIPS 140-2 compliant (NIST, 2012). It uses Active Directory to manage keys and provides for emergency access (Burchill, 2010). However, like BitLocker to Go, it does not have robust reporting capabilities and cannot provide the reports required to show compliance (Beaver, 2009). It is free if purchased with Windows 7 Enterprise or Ultimate Edition (Burchill, 2010). However, this requires organizations to purchase upgrades if they are running Windows 7 Professional, Home Premium, or Starter Edition.

There are two factors to consider when looking at a full-disk encryption solution. First, small businesses cannot be expected to run two different encryption packages since this can confuse users. A security researcher, Matt Bishop, states that configuration errors are the possible cause of more than 90% of computer security failures (Whitten and Tygar, 2005). A consistent interface and design are critical to ensuring that encryption solutions work correctly for regular users that need to use them because of security constraints (Whitten and Tygar, 2005). Second, the package should support reporting on fixed disks and USB flash drives in one module. Both the McAfee and Symantec solutions support this, while the Microsoft and TrueCrypt solutions are lacking (McAfee, 2012) (Symantec, 2012). The McAfee solution requires special USB flash drives, while the Symantec solution supports fixed disks, USB flash drives, and CD-ROM disks (McAfee, 2012) (Symantec, 2012).

It is due to these reasons that the Symantec solution is recommended for both USB and full-disk encryption. It meets the controls, and provides a consistent interface and reporting for both while allowing the customer freedom of choice to use whatever removable media they wish (Symantec, 2012).

Table 5: Fixed Disk Encryption Comparison Matrix

	Symantec PGP Encryption	**McAfee Endpoint Encryption**	**TrueCrypt**	**Microsoft BitLocker**
Cost	$154.00/year	$85.99/year	$0.00	$129.95-$169.95 for an upgrade
FIPS 140-2 Compliance	Yes	Yes	No	Yes
OS Support	Windows 2000-Windows 7, Windows Server 2003-2008 R2Linux, Mac OS X	Windows XP-Windows 7, Windows Server 2003-2008 Mac OS X	Windows 2000-Windows 7, Linux, Mac OS X	Windows 7 Ultimate, Windows 7 Enterprise, Windows Server 2008 R2
Automatic Key Management	Yes	Yes	No	Yes
Logging/Reporting	Yes	Yes	No	Does not provide proof of encryption
Recommended Solution	Yes	No	No	No

Technical Policy and Unique User Identification/Access Control

For Technical Policy, which governs the ability to configure PCs to meet a minimum set of security criteria by implementation and enforcement of configuration controls, and Unique User Identification/Access Control, two options were researched. The requirements for these were covered in Section B of the matrix. Those systems were Microsoft Active Directory Domain Services and Linux/Samba 4.

Microsoft Active Directory Domain Services comes standard with Windows Server, and provides a repository for configuration information, authentication requests, and information about the objects stored in it (Microsoft, 2012). It is designed to manage corporate identities, credentials, and system and application settings (Microsoft, 2012). It also allows users to manage users, computers, groups, printers, applications, and other objects from one centralized platform (Microsoft, 2012). One of the components of Active Directory Domain Services is Group Policy. It is used to manage configurations for groups of computers and users, including options for registry-based policy settings, security settings, software deployment, scripts, and preferences (Rock and Stephens, 2012).

Active Directory Domain Services and Group Policy satisfy controls B100, Workstation Logical/Physical Security and B101- Access Control in that when a machine is joined to Active Directory, there is centralized management of who can access that machine or not (Microsoft, 2012). Active Directory can also be configured to satisfy controls B103 – Audit Controls and B106 – Non-repudiation/Centralized Authentication because Microsoft Active Directory utilizes the Kerberos Protocol to provide a degree of non-repudiation through using the Kerberos protocol for client/server authentication communication, and through its use of event logs to document authentication attempts on the client and server sides (Kerberos Consortium, 2012) (Microsoft Support, 2006). Audit controls B102 – Unique User Identification and B104 – Person or Entity Authentication are supported through the creation of unique user accounts which can authenticate to Active Directory (Microsoft, 2012). Audit Control B105, Consistent Time is satisfied by the use of the Windows Time Service to provide time synchronization between PCs and an Active Directory server that synchronizes to an NTP time source (Microsoft, 2010). Control B107 – Document Updates is satisfied by the use of the Windows event log to document system and patch changes on each PC, which can be scripted and managed from a server (Microsoft TechNet, 2009).

Samba 4 is a Linux-based implementation of Microsoft's Active Directory and SMB/CIFS file and print-sharing protocols (Samba.org, 2012) (Edge, 2011). It is currently in beta stage (Edge, 2011). However, Samba has historically been used to provide a Free Software replacement to Microsoft's proprietary authentication systems so that true interoperability can be achieved (Samba.org, 2012). Many corporations have utilized Samba to provide a Free Software alternative to Windows Domains or Active Directory (Samba.org, 2012). However, Samba 4 requires the use of an NTP daemon on each client to synchronize time (Corbet, 2012). It also uses the UNIX logging format to log events and errors, which is not consistent with Windows (Eckstein, Collier-Brown, Kelly, 1999). It can log to text files and also to syslog (Kukkukk, 2012). However, adding users to Samba requires using the Linux command line to run commands to do so (Red Hat, 2012).

Due to the fact that Samba 4 is currently in beta stage, and has significant issues that need to be resolved before a release date can be finalized, controls B100 – Workstation Logical/Physical Security and B106 – Non-repudiation/Centralized Authentication cannot be satisfied because the product still has major issues preventing the use of it in a production environment. Therefore, the use of Samba, which is historically the Free Software alternative to Microsoft Windows Server and Active Directory, cannot be recommended. Microsoft Active Directory, which meets all of the required security controls, and has also been a proven product in the marketplace, is the recommended solution.

Table 6: Technical Policy Comparison Matrix

	Microsoft Active Directory	**Samba 4**
User Authentication	Yes	Yes
In Production	Yes	Beta, no certain release date
Requires additional software?	No	Yes, NTP needed to synchronize time
Requires command line to add users?	No	Yes
Logging in same format?	Yes	No
Management of machines and objects via Group Policy?	Yes	Beta
Non-repudiation of authentication requests?	Kerberos	Beta
Cost	Requires Windows Server License	Free
Recommended Solution	Yes	No

Proxy Server and Data Loss Prevention

To evaluate Proxy Server and Data Loss Prevention solutions three proxy server and three data loss prevention software options are available. They work to mediate Internet access and can help guard against potential breaches by ensuring that data is not transmitted insecurely. The requirements for these are covered in Section C of the matrix.

Proxy servers need to support the Internet Content Adaption Protocol (ICAP), which allows a web proxy to pass messages to another server to be modified in transit (Elson and Cerpa, 2003). There are three widely-used proxy servers on the market which support ICAP. They are the Blue Coat ProxySG 300, WebSense, and Squid, which is the Open Source solution (Blue Coat, 2012) (WebSense, 2012) (Rousskov, 2012). The Blue Coat proxy solution costs $5,785.00 plus yearly support costs (Edgeblue.com, 2012).

The WebSense solution costs $13,440.00 plus yearly user licenses and support for the appliance (SecureHQ.com, 2012). The Squid solution is Open Source, is bundled with many Linux distributions and firewall appliances, and is free (squid-cache.org, 2012). Due to the fact that many small to medium-sized businesses will not be able to afford the Blue Coat or WebSense solutions, and the Squid solution supports the same required features, this is the preferred solution for the proxy server.

Table 7: Proxy Server Comparison Matrix

	Blue Coat ProxySG 300	**WebSense**	**Squid**
ICAP Support	Yes	Yes	Yes
Cost	$5,785.00 + yearly support	$13,440.00 + yearly support	$0.00
Recommended Solution	No	No	Yes

For the Data Loss Prevention servers, the solution needs to support scanning e-mail, web proxy servers via ICAP, and endpoints via a local agent. It also needs to support user-configurable rules. This will help satisfy controls C100 – Transmission Security, C101 – Protection against unauthorized disclosure, and C102 – Device and Media Controls, by giving organizations the ability to prevent unauthorized disclosure via the use of data loss prevention software, and the ability to track the transfer of ePHI onto electronic media that can be removed from the facility. Symantec, McAfee, and myDLP offer solutions which meet the requirements. Symantec offers Symantec DLP-9, which is a smaller version of their larger DLP product that can interface with web proxy servers and has an endpoint client that reports into a central server (Craig, 2009). McAfee offers McAfee DLP Endpoint and McAfee DLP Prevent, which can be combined with ePolicy Orchestrator to form a DLP solution that handles web proxies and endpoints (McAfee, 2012). MyDLP offers a Linux-based virtual machine appliance that interfaces with ICAP-compliant web proxy servers, e-mail, has an endpoint client that reports back to the virtual machine, and is also Open Source (mydlp.com, 2012). The Symantec solution starts at a base price of $25,000 plus yearly support (Craig, 2009). The McAfee solution requires ePolicy Orchestrator, costs $29,800.00 for the software, $35,000 for the DLP appliance, and additional yearly costs for the ePolicy Orchestrator license and yearly support (Stephenson, 2007). All of these products support user-configurable rules (Craig, 2009) (Stephenson, 2007) (mydlp.com, 2012).

The myDLP solution offers the same basic features as the Symantec and McAfee solutions, but has the benefit of being Open Source and free for download. It provides the same features as the much more expensive Symantec and McAfee solutions at a much lower cost, and can use older hardware or a virtual machine to host it. MyDLP is the recommended solution due to its cost and support for all requirements.

Table 8: DLP Software Comparison Matrix

	Symantec DLP-9	**McAfee DLP Prevent**	**myDLP**
Cost	$25,000 + support	$29,800 for software, $35,000 for DLP appliance, and additional license costs	$0.00
Web Proxy Support	Yes	Yes	Yes
Endpoint Support	Yes	Yes	Yes
E-mail Support	Yes	Yes	Yes
Virtual Machine Support	Yes	No	Yes
Recommended Solution	No	No	Yes

Firewall

The requirements for a firewall solution were developed in Section D of the matrix. For selecting a firewall solution, there were three Open Source packages considered: PfSense, m0n0wall, and IPCop. These are all packages that are designed to take older PCs which are not capable of running Windows 7 and turning them into robust firewalls. A decent firewall should have robust logging, an Intrusion Detection System (IDS), and the ability to be configured to protect against unauthorized intrusions.

PFSense comes with the ability to integrate an Intrusion Detection System, Intrusion Prevention System, robust logging, and Squid Proxy with ICAP support into the base firewall system (squid-cache.org, 2012)(pfsense.org, 2012). IPCop has a decent firewall built in and the ability to log to multiple sources, but does not have IDS (Ipcop.org, 2012). M0n0wall has a firewall and robust logging, but does not have an integrated proxy or IDS (Buechler, 2008). Out of the three solutions, PFSense meets the stated requirements, which were D100 – Protection against unauthorized disclosure, D101 – Physical Safeguards, and D102- Integrity. It is the recommended solution.

Table 9: Firewall Appliance Comparison Matrix

	PFSense	**IPCop**	**M0n0wall**
Firewall	Yes	Yes	Yes
IDS	Yes	No	No
IPS	Yes	No	No
Logging	Yes	Yes	Yes
Squid Proxy with ICAP Support	Yes	No	No
Cost	$0.00	$0.00	$0.00
Recommended Solution	Yes	No	No

Antivirus

To select an Antivirus solution that would meet the requirements developed in Section E - Antivirus, the criteria used was a solution certified by an independent testing laboratory, ICSA Labs (ICSA Labs, 2012). ISCA Labs, a division of Verizon Business, publishes a list of certified Anti-Virus products (ICSA Labs, 2012). The only corporate anti-virus solution on their list of products was the AVG Anti-Virus Business Edition (ICSA Labs, 2012). Solutions from Symantec, McAfee, Trend Micro, and Kaspersky were all certified for home usage, but not for corporate use by ISCA Labs. This costs $89.99 for two machines per year, which averages out to $45 per machine (AVG.com, 2012). While there are other products out there that are supported in corporate environments, they have not undergone scrutiny by an independent testing laboratory. A certified solution means that the product will be able to adequately protect the environment against threats. The controls satisfied by an antivirus solution were E100 – Integrity, and E101 – Protection against unauthorized disclosure. The recommended solution is the AVG Anti-Virus Business Edition product.

Policies, Procedures, Risk/Impact Analysis, and Contracts

The most comprehensive set of requirements is in Section F – Policies, Procedures, Risk/Impact Analysis, and Contracts. This section of the matrix covers the required policies and procedures for securely implementing an EMR system within a medical facility. There are a significant amount of controls required to satisfy requirements here.

To satisfy them, a multi-faceted approach is recommended. First, the organization needs to engage the services of a consulting group focused on small to medium-sized businesses that can provide policy templates and advice, as well as risk assessment services (Long, 2011). It is recommended that the organization also customize the templates to meet the requirements of the organization and the issues discovered during the risk assessment. One of the organizations that performs these services, the Supremus Group, offers packages for organizations to not only provide policy templates, but also provides certification training for employees (Supremus, 2012).

Secondly, the organization needs to engage the services of a lawyer to review their contracts to ensure that the contracts that they have meet Business Associate Agreement rules, and that they can correct any compliance issues (Tovino and Reisz, 2012). Additionally, the organization must ensure that their policies meet requirements. Next, they need to train and empower a staff member to look over logs and check for and help resolve compliance issues. This would be the equivalent of a CISO for a smaller business (Long, 2011). The computer systems in place will generate log files and warnings, and it is a requirement to monitor those. It is also a requirement to document changes, and not documenting them is a compliance issue. Therefore, it is important, even if the person is part-time on the task, to have someone dedicated to compliance, and empower him or her to ensure that the organization does what is required. The HIPAA Security Rule mandates this review process, and Long’s article further underscores that need.

Finally, a lawyer or other qualified professional with an understanding of the HIPAA Security Rule should review the proposed solution to ensure that it really does meet the stated requirements. It is key to understand how the operations of a remotely hosted system operate and prove the solution is compliant by matching known criteria and their contracts.

Proof of Concept Implementation

As part of this project, a small proof of concept solution was developed using the pfSense firewall and myDLP Data Loss Prevention software. This was put together to prove that the recommended software would work in a small office environment. A Dell Dimension 3000 with 512 megabytes of RAM, an eighty gigabyte hard drive, and two network cards were used to house the pfSense firewall. A Dell Dimension 3000 with 768 megabytes of RAM and an eighty gigabyte hard drive were used to house the myDLP Data Loss Prevention server. The myDLP server was connected to the firewall on a switched network. The firewall was connected to a Comcast cable connection.

The pfSense solution is packaged as a CD image. This was downloaded from their web site and burned to a CD. The Dell Dimension was then booted to the CD. Installation of the software to the hard drive took approximately ten minutes. Configuration of the software, including specifying IP addresses and basic firewall rules, took approximately thirty minutes. Updating the software to the latest version and installing the Snort IDS/IPS and Squid proxy caching software took another thirty minutes. Configuring Squid for ICAP proxy access took another five minutes. The result was a firewall appliance that had a full IDS and IPS, along with an ICAP-compliant proxy server.

The myDLP solution is also packaged as a CD image based on Ubuntu Linux. This was also downloaded from their web site and burned to a CD. The other Dell Dimension was booted from it, and the software was installed from it. It took approximately thirty minutes to install the software and assign an IP address to the server. It took thirty minutes to configure myDLP using an online tutorial and its web-based interface to accept traffic from the pfSense server, have a basic rule set in place to monitor for Social Security Numbers and credit card numbers, and block their transfer via the web or to a USB flash drive. Installation of the client on a Windows 7 PC on the same network required the use of a Microsoft Installer package and development of a small script to point the workstation to the myDLP server.

The result here was an endpoint solution which is capable of examining data transfer from a workstation, and is able to block and log potential breaches. The solution was implemented using lower-cost hardware which is not capable of running Windows 7. The software was capable of detecting social security numbers and credit card numbers, and was able to block their unencrypted transfer over the Internet and to a USB flash drive plugged into a PC running the myDLP client.

Recommended Implementation Strategy

The implementation of any EHR or EMR system is a complex task. The road toward successful implementations has been marked by failures large and small. Cloud Computing adds on another level of complexity and security to the process. The recommendation for small to medium-sized medical practices that would like to reap the economic benefits of cloud-based EMR or EHR systems is to start by utilizing the HIPAA/HITECH/Breach Notification Rule/ONC-ATCB matrix to guide their compliance efforts internally. The purposes of this tool are to understand the real risks, and to mitigate them before attempting to shift the risk to someone else's system. While an Electronic Medical Records system in the cloud may be fully in compliance with

ONC-ATCB regulations, but the usage of a virus-infected PC on a Linksys router, or an insecure wireless access point at Starbucks is not. There is no magical “cloud dust” to make the organization secure and “get your money!”, as much as some of the ads out there would like to tell you otherwise (Longwood Systems, 2012).

The recommended implementation strategy consists of several parts. The goal here is to list the steps so that a small to medium-sized organization can easily implement and spread the costs across a period of time, and develop a security process, not just a point solution to implement Cloud. The implementation of an Electronic Medical Records system can be very costly and time-consuming. The goal is to provide understanding of the processes and a gradual implementation of a new cloud-based system so that it meets rules and regulations. The end goals, however, are security and protection of patient data.

The first step is to train the workforce. HIPAA and HITECH training from a reputable training company will provide the workforce with the understanding of what to do, what the penalties are, and most importantly, sets expectations as to how to perform (Long, 2011). The article “Hand Hygiene Compliance Among Health Care Staff and Student Nurses in a Mental Health Setting”, by Marilyn Ott, RN, BScN, MScN, and Rachel French, RN, discusses a similar compliance issue which healthcare providers are dealing with, which is hand washing compliance for infection control. Ott and French discuss an approach where positive behavior modeling is used with continual training and cultural reinforcement, along with visual aids to provide an effective approach to compliance improvement in the healthcare environment (Ott, 2009).

Providing training as opposed to creating a culture of fear will reduce errors and provide understanding of the HIPAA Privacy and Security rules. The article "Brief Reports: The Impact of Fear of HIPAA Violation on Patient Care", by Bryan K. Touchet, M.D., Stephanie R. Drummond, D.O., and William R. Yates, M.D, touches on the fact that easily preventable errors have occurred because of fear of violating HIPAA, failure to understand the HIPAA Privacy Rule, and ethical concerns about HIPAA (Touchet, 2004). Training costs can range from $25.00 per person for online training costs from Evolve Healthcare Training, to $2,700 per person for in-person training from the Supremus Group (Evolve Healthcare Training, 2012) (Supremus, 2012).

The recommendation is to train the workforce using a reputable consulting firm that understands the HIPAA Privacy and Security rules, and the HITECH Act. The goal is to build a culture of positive reinforcement. The more understanding there is of what to do, the less fear will exist. Positive reinforcement is much more effective than punitive reinforcement (Ott, 2009).

Secondly, it is recommended that the organization contact an attorney or legal counsel that can help them review their contracts, business associate agreements, policies, and procedures to ensure they are in compliance with the HIPAA Security Rule and HITECH, as there are major changes which can affect the organization (Tovino and Reisz, 2012). The organizational policies of the business should be updated to reflect required changes with HIPAA and HITECH, and that the changes are socialized with the entire workforce (Long, 2011). The Digital Business Law Group charges between

$5,000 and $7,500 for a HIPAA audit that includes recommended changes to these agreements, policies, and procedures (Digital Business Law Group P.A., 2012).

Next, the security recommendations should be implemented internally in the office on the computers. The goal is to ensure that the computers which will be accessing the cloud computing solution are protected from malware via an antivirus implementation, have current security patches, are encrypted, have protection against unencrypted data being lost via USB drives or stolen/lost PCs, and that each user has a unique username and password to authenticate to resources internally. A powerful network firewall solution should be implemented. Data Loss Prevention software is also recommended to track PHI as it enters and leaves the office environment, and to block any potential breaches. The goal will get the organization to a point where the computers themselves will have a significantly higher degree of protection, will be in compliance with HIPAA, HITECH, Breach Notification Rule, and ONC-ATCB regulations, and will get them ready to use remotely hosted services.

Furthermore, organizations should have a comprehensive plan for standardizing and upgrading their hardware from three to five years so that they can run current software and enjoy the benefits of the latest protection methods (Ray, 2009). The instrument should be used as a continual compliance checklist for the organization going forward in combination with training. It is important that the organization be aware of the rules, and has a quick reminder of how to stay in compliance. The organization should hire a consultant to conduct a risk assessment and a Business Impact Analysis (BIA), as this is required by the HIPAA Security Rule and Meaningful Use regulations (Long, 2011). A plan should address the outstanding risks in the risk assessment.

(Medicare and Medicaid Programs, 2010). Using the Business Impact Analysis calculator from continuitycompliance.org, a BIA for a business with 10-49 employees, $2.5 million in revenue, and twenty critical business processes will require 76.75 hours of work for a full BIA (ContinuityCompliance.org, 2012). A consultant, at a rate of $100 per hour, will cost $7675 to perform this engagement.

Fourth, the organization should utilize the compliance instrument developed as part of an initial vendor selection process for a cloud-based EMR/EHR system. The small to medium-sized providers should do their own search for ONC-ATCB certified providers who meet their business needs, starting with the CCHIT website, and proceed to use the instrument to determine who meets HIPAA Security Rule, HITECH, Breach Notification Rule, and ONC-ATCB certification requirements.

Fifth, the organization should utilize the set of providers that comes from the initial selection process to find a vendor that meets their requirements and provides a supportive workflow (Miller and Sim, 2004). This will help make a decision that is based upon more than a presentation. The organization should also retain an attorney to go over the vendor contracts and make sure that everything meets Business Associate Agreement requirements. This can cost $100 to $500 an hour, depending upon the complexity of the contract and the skill of the lawyers (Costhelper.com, 2012).

Sixth, the organization should make a decision and implement an EMR system based on the selection process. Using both the compliance instrument and their selection workflow, they should find a system that meets their workflow and security requirements.

Seventh, organizations should develop and maintain a list of metrics to monitor continually such as system uptime, help desk response time, application performance, number of breaches, and report performance (Eckerson, 2011). Organizations should review these metrics monthly to gauge performance of the system, and the level of customer support they are receiving (Eckerson, 2011).

Eighth, organizations should be continually vigilant about their risk. Being a smaller provider does not exempt anyone from risk assessments (HIPAA Administrative Simplification, 2006). The organization should use a consulting firm or legal counsel to assist in performing regular risk assessments to demonstrate compliance with the HIPAA Security Rule. A staff member should be empowered to review systems access on both the cloud-based system and locally to continually evaluate compliance (HIPAA Administrative Simplification, 2006). Kirk Nahra, in his article “HIPAA Security Enforcement is here”, recommends that companies pay close attention to public security breach reports, and continually assess policies and procedures to ensure compliance (Nahra, 2008).

The end product from this eight-step implementation recommendation strategy is that a smaller organization can use cost-effective means to effectively implement the security controls required by the HIPAA Security Rule, HITECH, Breach Notification Act, and ONC-ATCB certification for a cloud-based EMR. This will effectively save the organizations running their own in-house EMR system and will put security controls in place that will make the organization as a whole more secure. This prevents organizations from the potential risks caused by having false hope that an EMR implementation will solve all of their issues.

Benefits

There are several benefits of implementing the cloud-based Electronic Medical Records system utilizing the process and strategy developed. There is also one drawback, which is the potential overall cost. The benefits, however, are far-reaching.

The first benefit is a framework for organizations to be compliant, according to federal law. The strategy does not focus on a sudden implementation, but a framework for getting compliant using positive reinforcement, methodical steps, and mitigating risk at all levels.

The second benefit is that organizations will be able to provide evidence of compliance to the required federal agencies to receive Meaningful Use financial incentives for the implementation of a cloud-based EMR/EHR system. The augmentation and design of a network using lower-cost tools using our reference design, combined with the use of the instrument developed, should provide organizations with the information they need to not only be compliant on the EMR side, but in their office as well.

In addition to Meaningful Use financial benefits, there are also operational benefits to the organization as well. The article ”A Cost-benefit Analysis of Electronic Medical Records in Primary Care”, from The American Journal of Medicine, cites an estimated net benefit of $86,400 for a provider for a five year period when an organization implements Electronic Medical Records (Wang et al, 2003).

Miller and Sim, in their article “Physicians’ Use of Electronic Medical Records: Barriers and Solutions”, also cite the operational benefits of implementing EMR. They specifically cite that it allows physician practices to pursue more powerful quality-improvement programs than possible with paper-based records (Miller and Sim, 2004).

However, they indicate that the quality improvements depend heavily on the use of the EMR to accomplish key tasks (Miller and Sim, 2004).

The next benefit is that the implementation of this framework will provide organizations with insight into what data they have, how it is transferred, and where the risk lies with potential breaches. The implementation of a Data Loss Prevention system will provide organizations with an understanding of where their data goes. The organization will be more secure than before since they will be able to track their data and avoid potential breaches. Furthermore, this implementation of the required controls provides the organization with accurate logging track information of what data they own and what is being transferred.

The final benefit is that following the strategy will increase the overall security of the organization. Where an EMR is hosted is only part of the picture. The other part is what machines access it, and how they are secured. Even if there is encryption and security on a cloud-based system, the biggest weakness is still the endpoint. Increasing the security of the endpoints and how they are managed helps mitigate larger risks to the organization.

While there is a cost to implementing any Electronic Health Record or Electronic Medical Record system, there is also conversely the threat of being paid less by Medicare for not implementing such a system (Medicare and Medicaid Programs, 2010). Usage of a cloud-based system costs significantly less than trying to implement a product in-house. The goal of what was done here is to implement such a system and meet security controls.

Lessons Learned, Suggestions, and Conclusion

The most important lesson learned is that security around cloud-based systems involves a lot more than just the cloud-based system. Everything which needs to access the EMR needs to be as secure as it, as well as the policies and procedures governing its use. There are multiple security criteria surrounding any machine that contains Protected Health Information, not just the EMR. The biggest potential security hole may be the workstations themselves, and there is not clarity between the HIPAA Security Rule, HITECH Act, and the Breach Notification Rule with regards to encryption. The ONC-ATCB regulations for certified EMR/EHR systems provided the required clarity with regards to encryption and security, however.

Any organization that wants to connect to the cloud for their business requirements needs to get their house in order first by implementing required policies and procedures, and putting a network in place that is capable of handling the security requirements on multiple levels (Long, 2011). A lost USB flash drive that may contain patient information could have devastating financial and reputational consequences for small to medium-sized organizations (Nahra, 2008).

The group of cloud-based providers should be more realistic with their customers. Many advertisements indicated how much money an organization could make by implementing an electronic medical records system, as opposed to how the solution could provide benefit to the organization as part of an overall security package. Providers should be realistic as to the amount of training required to implement an EMR. The Department of Health and Human Services should be clear on customer expectations.

Many systems which advertise themselves to be HIPAA compliant are not. In particular, the GE Radiology Information System that was implemented at Temple

University Hospital used unique user names and passwords for the end users, but not for the GE technical support staff or the system services. Internal Auditors flagged this as part of a routine post-implementation audit. This means that this particular vendor will need to redesign a multi-million dollar system and their internal support processes to be in compliance with the HIPAA Security Rule.

Another example is a Meaningful Use risk assessment for a community hospital located in Philadelphia. This hospital, to save costs, utilized an Application Service Provider for their EMR system. A CPA firm was engaged to provide a privacy and security assessment of the third-party vendor. As part of this engagement, two findings were discovered. The first was that the vendor had not filed a SAS 70 or SOC 2 privacy and security controls report for several years. Secondly, upon further research, it was discovered that the company was granting unauthorized users access to the databases that contained protected health information of its customers with no need to know.

Staff needs to be made aware that even though a software package may be HIPAA-compliant, the installation and configuration of the package may not be if the system itself is configured with generic accounts. As part of the audit of the Medhost Emergency Department Information System at Temple University Health System, the sole finding found was a procedural issue where generic usernames were given out to staff to view data in an otherwise completely compliant system. Internal Audits went to several departments to find out that user rights were improperly assigned. Several departments had to change how user access was provisioned based upon this finding.

Implementing a Data Loss Prevention system takes more work than just dropping something on the network and being punitive toward end users. Much of the implementation time requires speaking with the stakeholders and training the end users. There has to be education including a training program, and there needs to be time spent hand-holding with the users. Security controls cannot simply be implemented and expected to work without training and sitting in the line of fire with customers.

It is entirely possible for a small to medium-sized healthcare organization to implement a cloud-based EMR that meets HIPAA, HITECH, Breach Notification Rule, and ONC-ATCB guidelines; it is a solution that can save organizations money as opposed to running an EMR in-house. However, the issue is that the organizations need to lock down and secure the PCs that will access the EMR first, get their own policies, procedures, and contracts in order, and continually monitor their own systems for uptime, and themselves for compliance.

Small to medium-sized providers will need to use a robust systems selection process to vet cloud-based systems based on their conformance to the required federal guidelines. They need a strategy based upon a systemic implementation of training, contract analysis, risk assessment, technology implementation in the office, vendor selection, and monitoring.

Technology in healthcare is a reachable goal, even with all the regulations out there. There is a lot of confusion and misunderstanding as to what to do. There are many Cloud vendors who are not secure. The goal is to help organizations avoid them, implement secure solutions, and continually stay compliant.

References

AllScripts Corporation (Allscripts) (2012). System Environment Specifications Network PC, Peripheral& Server Requirements. Retrieved on April 8, 2012 from http://www.allscripts.com/content/dam/allscripts/documents/MyWay_8.6_SystemEnvironmentSpecs.pdf

American Institute of Certified Public Accountants (AICPA) (2011, May 1). Service Organizations. Applying SSAE No. 16, Reporting on Controls at a Service Organization (SOC 1), New York, NY: AICPA.

Armbrust, Michael et al. (2010). A View of Cloud Computing. Communications of the ACM, April 2010, Volume 53, No. 4, pp. 50-58.

AVG.com (2012). AVG Anti-Virus Business Edition 2012. Retrieved on April 12, 2012 from http://www.avg.com/us-en/antivirus-business

Beaver, Kevin (2009). Considerations for BitLocker in Microsoft Windows 7. Retrieved on April 8, 2012 from http://www.principlelogic.com/docs/BitLocker_in_Windows7.pdf

Beck, Micah, Moore, Terry, Plank, Jim, Swany, Martin (2012). Logistical Networking: Sharing More Than the Wires. Retrieved on March 16, 2012 from http://loci.cs.utk.edu/ibp/files/pdf/LogisticalNetworking.pdf

Biswas, Kamanashis, and Islam, Md. Ashraful (2009). Hardware Virtualization Support in Intel, AMD, and IBM POWER Processors. (IJCSIS) International Journal of Computer Science and Information Security, Vol 4, No. 1 & 2, Retrieved on March 10, 2012 from http://arxiv.org/pdf/0909.0099.pdf

Blue Coat (2012). Blue Coat Full Proxy Edition –ProxySG 300/600. Retrieved on April 9, 2012 from http://www.edgeblue.com/datasheets/Blue_Coat_ProxySG_300-600_Full_Proxy.2.pdf

Blue Coat (2012). ICAP Data Trickling. Retrieved on April 9, 2012 from http://www.bluecoat.com/sites/default/files/product_tech_primers/ICAP_Data_Trickling.7.pdf

Breach Notification for Unsecured Protected Health Information (2009), 74 Fed. Reg. 42740 (to be codified in 45 CFR parts 160 and 164).

Buechler, Chris (2008). M0n0wall Handbook. Retrieved on April 10, 2012 from http://doc.m0n0.ch/handbook/

Burchill, Alan (2010, September 1). Best Practice: How to use Group Policy to save "BitLocker to Go" recovery keys in Active Directory – Part 1. Retrieved on March 15, 2012 from http://www.grouppolicy.biz/2010/01/how-to-use-group-policy-to-save-bitlocker-to-go-recovery-keys-in-active-directory-part-1/

CDW.com (2012). McAfee Endpoint Encryption for PCs – license. Retrieved on April 8, 2012 from http://www.cdw.com/shop/products/McAfee-Endpoint-Encryption-for-PCs-license/1439970.aspx

CDW.com (2012). Search Results for McAfee USB Drives. Retrieved on April 8, 2012 from http://www.cdw.com/shop/search/result.aspx?key=mcafee+usb+drives&wclsscat=&b=&p=&searchscope=All&ctlgfilter=&sr=1

CDW.com (2012). Symantec Endpoint Encryption Removable Storage Edition (v. 8.2) – license. Retrieved on April 8, 2012 from http://www.cdw.com/shop/products/Symantec-Endpoint-Encryption-Removable-Storage-Edition-v.-8.2-licen/2495745.aspx

Center for Medicare and Medicaid Services (CMS) (2012). CMS EHR Meaningful Use Overview EHR Incentive Programs. Retrieved on March 5, 2012 from https://www.cms.gov/EHRIncentivePrograms/30_Meaningful_Use.asp

Center for Medicare and Medicaid Services (CMS) (2012). HealthIT.hhs.gov: Electronic Medical Records. Retrieved on March 1, 2012 from http://healthit.hhs.gov/portal/server.pt/community/electronic_medical_records/1219/home/15591

Certification Commission for Health Information Technology (CCHIT) (2012). About the Certification Commission for Health Information Technology. Retrieved on March 1, 2012 from http://www.cchit.org/about

Certification Commission for Health Information Technology (CCHIT) (2012). What is the ONC-ATCB 2011/2012 Certification Program? Retrieved on March 1, 2012 from http://source.cchit.org/web/source/source-more

Certification Commission for Health Information Technology (CCHIT) (2012). CCHIT Certified 2011. Retrieved on March 1, 2012 from http://www.cchit.org/get_certified/cchit-certified-2011

Certification Commission for Health Information Technology (CCHIT) (2012). What is EACH?. Retrieved on March 1, 2012 from http://each.cchit.org.

Center for Medicare and Medicaid Services (CMS) (2012). HIPAA Administrative Simplification Statute and Rules. Retrieved on March 3, 2012 from http://www.hhs.gov/ocr/privacy/hipaa/administrative/index.html

Cerner Corporation (Cerner) (2012). Cerner and HP. Retrieved on April 8, 2012 from http://cerner.com/About_Cerner/Partnerships/HP/?LangType=1033

Chen, Yanpei, Paxson, Vern, and Katz, Randy H. (2010, January 20). What's New About Cloud Computing Security? Retrieved on March 7, 2012 from http://www.utdallas.edu/~mxk055100/courses/cloud11f_files/what-is-new-in-cloud-security.pdf

City of Philadelphia (phila.gov) (2012). Phila.gov | Public Health, Division of Disease Control, Epidemiology Program. Retrieved on February 5, 2012 from http://www.phila.gov/health/DiseaseControl/Epidemiology.html

Congdon, Kenneth (2009). How Much Will an EHR System Cost You? Healthcare Technology Online. Retrieved on March 1, 2012 from http://www.healthcaretechnologyonline.com/article.mvc/How-Much-Will-An-EHR-System-Cost-You-0001

ContinuityCompliance.org (2012). Business Impact Analysis Calculator. Retrieved on April 12, 2012 from http://www.continuitycompliance.org/tools-resources/community-projects/business-impact-analysis/

Corbet, Jonathan (2012, January 16). LCA: A Samba 4 Update. Retrieved on April 8, 2012 from http://lwn.net/Articles/475592/

Costhelper.com (2012). How much does a licensing contract cost? Retrieved on April 12, 2012 from http://smallbusiness.costhelper.com/licensing-contract.html

Cox, S, Wilcock, P and Young, J (1999). Improving the repeat prescribing process in a busy general practice. A study using continuous quality improvement methodology. *Qual Health Care* 1999;**8**:119-125 doi:10.1136/qshc.8.2.119

Cristiano, J. J., Liker, J. K. and White, C. C. (2000), Customer-Driven Product Development Through Quality Function Deployment in the U.S. and Japan. Journal of Product Innovation Management, 17: 286–308. doi: 10.1111/1540-5885.1740286

Department of Homeland Security (DHS) (2012). Business Impact Analysis | Ready.gov. Retrieved on March 12, 2012 from http://www.ready.gov/business-impact-analysis

Department of Homeland Security (DHS) (2012). Risk Assessment | Ready.gov. Retrieved on March 12, 2012 from http://www.ready.gov/risk-assessment

DeFelice, Alexandra (2010). Cloud Computing: What Accountants Need to Know. Journal of Accountancy, November, 2010. Retrieved on March 1, 2012 from http://sju.com/documents/cloud_computing_what_accountants_need_to_know.pdf

Dell Corporation (Dell) (2012). Dell Poweredge T110 II. Retrieved on April 8, 2012 from http://configure.us.dell.com/dellstore/config.aspx?oc=bedt5dd&c=us&l=en&s=bsd&cs=04&model_id=poweredge-t110-2&

Digital Business Law Group, P.A. (2012). HIPAA/HITECH Audit. Retrieved on April 12, 2012 from http://www.digitalbusinesslawgroup.com/ps-hipaa-audit.html

Eckerson, Wayne W (2011). Performance Dashboards: Measuring, Monitoring, and Managing Your Business. Hoboken, NJ: Wiley and Sons

Eckstein, Robert, Collier-Brown, David, and Kelly, Peter (1999, November). Using Samba – 4.8 Logging Configuration Options. Retrieved on April 8, 2012 from http://oreilly.com/openbook/samba/book/ch04_08.html

Edge, Jake. Releasing Samba 4. Retrieved on April 8, 2012 from http://lwn.net/Articles/469792/

Edgeblue.com (2012). Blue Coat SG300 Series Appliances. Retrieved on April 9,2012 from http://www.edgeblue.com/SG300.asp

Elson, J. and Cerpa, A (2003, April). RFC 3507 - Internet Content Adaption Protocol (ICAP). Retrieved on March 15, 2012 from http://tools.ietf.org/html/rfc3507

Epic Systems, Inc. (Epic Systems) (2012). Epic: Departments and Ancillaries. Retrieved on March 1, 2012 from http://www.epic.com/software-ancillaries.php

Evolve Healthcare Training (2012). Buy Online Training Courses Now! Retrieved on April 12, 2012 from http://www.ehipaatraining.com/orderpage.htm

Foley, Mary Jo (2010, February 26). Behind the IDC data: Windows still No. 1 in server operating systems. Retrieved on April 8, 2012 from http://www.zdnet.com/blog/microsoft/behind-the-idc-data-windows-still-no-1-in-server-operating-systems/5408

Geisinger Health System (Geisinger) (2012). PowerPoint Presentation on EMR System Implementation. Retrieved on March 1, 2012 from www.academyhealth.org/files/HIT/**Geisinger**%20Slides.pdf

George, Randy (2009, August 1). Rolling Review: Symantec ‘s DLP-9. Retrieved on April 9, 2012 from http://www.informationweek.com/news/security/attacks/218900115

Giglio, Peggy and Ingram, Julie (2012). Critical Features of an EMR System. Retrieved on March 28, 2012 from http://www.defran.com/_pdf/whitepapercriticalfeatures.pdf

Gokavarapu, Nageswararao V. and Banerjee, Shubhendu (2011, March 8). Virtualization Technologies for Agile Software Development. Retrieved on March 8, 2012 from http://public.dhe.ibm.com/software/dw/aix/au-virtualizationagile-pdf.pdf

Google, Inc., (2012). Google Message Encryption and the new HIPAA Legislation. Retrieved on March 1, 2012 from *http://*www.google.com/postini/pdf/hipaa_encryption.pdf

Government Printing Office (GPO) (2009). American Recovery and Reinvestment Act of 2009. Retrieved on March 4, 2012 from http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:h1enr.pdf

Hawthorn, Nigel (2009, November 5). Finding security in the cloud. Retrieved on March 31, 2012 from http://dx.doi.org.libproxy.temple.edu/10.1016/S1361-3723(09)70131-9

Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology (HIT) 75 Fed. Reg 44617.

HIPAA Administrative Simplification. 45 C.F.R. Pt. 160 (2006)

HIPAA Administrative Simplification: Enforcement (2009), 74 Fed. Reg. 56123.

Health Information Technology Standards Panel (HITSP) (2012). About Healthcare Information Technical Panel – Mission, Leadership, History, Retrieved on March 1, 2012 from http://www.hitsp.org/about_hitsp.aspx

Health Information Technology Standards Panel (HITSP) (2009). HITSP Collect and Communicate Security Audit Trail Transaction. Retrieved on February 4, 2012 from http://www.hitsp.org/ConstructSet_Details.aspx?&PrefixAlpha=3&PrefixNumeric=15

Health Information Technology Standards Panel (HITSP) (2009). HITSP Secure Communication Channel Transaction. Retrieved on February 4, 2012 from http://www.hitsp.org/ConstructSet_Details.aspx?&PrefixAlpha=3&PrefixNumeric=17

Health Information Technology Standards Panel (HITSP) (2009). HITSP Consistent Time Transaction. Retrieved on February 4, 2012 from http://www.hitsp.org/ConstructSet_Details.aspx?&PrefixAlpha=3&PrefixNumeric=16

Health Information Technology Standards Panel (HITSP) (2009). HITSP Entity Identity Assertion Component. Retrieved on February 4, 2012 from http://www.hitsp.org/ConstructSet_Details.aspx?&PrefixAlpha=4&PrefixNumeric=19

Health Information Technology Standards Panel (HITSP) (2009). HITSP Nonrepudiation of Origin Component. Retrieved on February 4, 2012 from http://www.hitsp.org/ConstructSet_Details.aspx?&PrefixAlpha=4&PrefixNumeric=26

Humboldt University Informatik (2012). Programming the Linksys WRT54GS Broadband Router. Retrieved on March 15, 2012 from http://sarwiki.informatik.hu-berlin.de/Programming_the_Linksys_WRT54GS_Wireless_Broadband_Router

ICSA Labs (2012). About ISCA Labs. Retrieved on April 9, 2012 from https://www.icsalabs.com/about-icsa-labs

ICSA Labs (2012). ICSA Labs Certified Products – Anti-Virus, Windows 7. Retrieved on April 9, 2012 from https://www.icsalabs.com/products?tid%5B%5D=4216&tid_3%5B%5D=4516&.x=14&.y=19

Ipcop.org (2012). IPCop v2.0.0 Administration Manual. Retrieved on April 10, 2012 from http://www.ipcop.org/2.0.0/en/admin/html/

Kangas, Eric, Ph. D. (2012). Gmail – not HIPAA Compliant Email – LuxSci FYI. Retrieved on March 1, 2012 from http://luxsci.com/blog/gmail-not-hipaa-compliant-email.html

Kerberos Consortium (2012). The Role of Kerberos in Modern Information Systems. Retrieved on April 8, 2012 from http://technet.microsoft.com/en-us/library/cc773013(WS.10).aspx

King, Leo (2011, November 22). Nasdaq Out of Date Software Helped Hackers Report. Retrieved on March 28, 2012 from http://www.csoonline.com/article/694804/nasdaq-out-of-date-software-helped-hackers-report

Kukkukk, Gunter (2012, March 7). [Samba] User audit logging. Retrieved on April 8, 2012 from https://lists.samba.org/archive/samba/2012-March/166517.html

Kumar, Sameer and Aldrich, Krista (2010). Overcoming barriers to electronic medical record (EMR) implementation in the US healthcare system: A comparative study. Health Informatics Journal 2010 16: 306. DOI: 10.1177/1460458210380523

Long, Kurt (2011, July). Proactive Defense. Retrieved on April 2, 2012 from http://www.hhnmag.com/hhnmag_app/jsp/articledisplay.jsp?dcrpath=TRUSTEEMAG/Article/data/07JUL2011/1107TRU_aboveboard_PracticalMatters&domain=TRUSTEEMAG

Longwood Systems, Inc. (2012). Longwood Systems, Inc. | Solutions | Electronic Medical Records. Retrieved on April 1, 2012 from http://www.longwoodsystems.com/medicalrecords.html

Marchany, R.C and Tront, J.G. (2002). E-commerce Security Issues. Retrieved on March 31, 2012 from http://dx.doi.org/10.1109/HICSS.2002.994190

McAfee Corporation (McAfee) (2012). Data Sheet – McAfee Endpoint Encryption. Retrieved on April 8, 2012 from http://www.mcafee.com/us/resources/data-sheets/ds-endpoint-encryption.pdf

McAfee (2012). McAfee DLP Prevent. Retrieved on April 9, 2012 from http://www.mcafee.com/us/resources/data-sheets/ds-dlp-prevent.pdf

McAfee Corporation (2012). McAfee Encrypted USB. Retrieved on April 8, 2012 from http://www.mcafee.com/us/resources/data-sheets/ds-encrypted-usb.pdf

McAfee Corporation (2012). McAfee ePolicy Orchestrator System Requirements. Retrieved on April 8, 2012 from http://www.mcafee.com/us/products/epolicy-orchestrator.aspx#=vtab-Requirements

Medicare and Medicaid Programs; Electronic Health Record Incentive Program; Final Rule (2010), 75 Fed. Reg. 44314.

Mell, Peter, and Grance, Tim (2009, October 7). Effectively and Securely Using the Cloud Computing Paradigm. Retrieved on March 31, 2012 from http://bing.exp.sis.pitt.edu:8080/webdav/cloud_resources/cloud_computing_112111/cloud-computingNISTpresentation.pdf

MessageLabs, Inc. (MessageLabs) (2012). Configuring Proxy Settings using Group Policy Management. Retrieved on March 15, 2012 from http://images.messagelabs.com/help/en-us/content/web_security_services/configuring_proxy_settings_using_group.htm

Microsoft Corporation (Microsoft). (2010, May 3). Best Practices for BitLocker in Windows 7. Retrieved on March 15, 2012 from http://technet.microsoft.com/en-us/library/dd875532(v=ws.10).aspx#BKMK_gpsettings

Microsoft Corporation (Microsoft) (2012). BitLocker Drive Encryption. Retrieved on April 8, 2012 from http://windows.microsoft.com/en-US/windows7/products/features/bitlocker

Microsoft Corporation (Microsoft). (2011, March 19). Create an SMTP Send Connector. Retrieved on March 15, 2012 from http://technet.microsoft.com/en-us/library/aa997285.aspx

Microsoft Corporation (Microsoft) (2012). Hardware and Software Requirements for SQL Server 2012. Retrieved on April 8, 2012 from http://msdn.microsoft.com/en-us/library/ms143506.aspx

Microsoft Corporation (Microsoft) (2010, March 12). How the Windows Time Service Works. Retrieved on April 8, 2012 from http://technet.microsoft.com/en-us/library/cc773013(WS.10).aspx

Microsoft Corporation (Microsoft) (2010, July 1). How to use Windows Software Update Services to deploy definition updates to computers that are running Windows Defender. Retrieved on March 15, 2012 from http://support.microsoft.com/kb/919772

Microsoft Corporation (Microsoft) (2012). Windows Server 2008 R2 Active Directory Overview. Retrieved on April 8, 2012 from http://www.microsoft.com/en-us/server-cloud/windows-server/active-directory-overview.aspx

Microsoft Corporation (Microsoft) (2012). Windows Small Business Server Overview. Retrieved on March 15, 2012 from http://www.microsoft.com/en-us/server-cloud/Windows-Small-Business-Server/overview.aspx

Microsoft Store (2012). Windows Anytime Upgrade. Retrieved on April 8, 2012 from http://www.microsoftstore.com/store/msstore/list/parentCategoryID.44066700/categoryID.50726200

Microsoft Support (2006, October 31). How to configure Active Directory diagnostic event logging in Windows Server 2003 and Windows 2000 Server. Retrieved on April 8, 2012 from http://support.microsoft.com/kb/314980

Microsoft Technet (2009, October 7). Identify Patches/Hotfixes installed on a computer on a given date. Retrieved on April 8, 2012 from http://gallery.technet.microsoft.com/scriptcenter/5aedad0f-753b-43e8-bd3f-fdbbccb64256

Miller, Robert H., and Sim, Ida (2004, March). Physicians' Use of Electronic Medical Records: Barriers and Solutions. doi: 10.1377/hlthaff.23.2.116 *Health Aff March 2004 vol. 23 no. 2 116-126*

Mohamed, Arif (2009). A History of Cloud Computing. Retrieved on March 6, 2012 from http://www.computerweekly.com/feature/A-history-of-cloud-computing

Nahra, Kirk J. (2008, November/December). HIPAA Security Enforcement is here. Retrieved on April 1, 2012 from http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4753677

National Institute of Standards and Technology (NIST) (2012). Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules. Retrieved April 8, 2012 from http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2010.htm#1332

NetMarketShare (2012). Top Operating System Share Trend – May 2011 to March 2012. Retrieved on April 8, 2012 from http://www.netmarketshare.com/os-market-share.aspx?qprid=9

Newegg.com (2012). Lexar JumpDrive FireFly 4GB USB 2.0 Flash Drive Model LJDFF4GBASBNA. Retrieved on April 8, 2012 from http://www.newegg.com/Product/Product.aspx?Item=N82E16820191278s

Office of the National Coordinator for Health Information Technology (ONC-HIT) (2012). Reference Grids for Meaningful Use or Standards and Certification Criteria Final Rules. Retrieved from http://healthit.hhs.gov/portal/server.pt?open=512&mode=2&objID=3584 on March 1, 2012

Oracle Corporation (2012). Oracle 2012 Technology Price List. Retrieved on April 01, 2012 from http://www.oracle.com/us/corporate/pricing/technology-price-list-070617.pdf

Ott, French (2009). Hand Hygiene Compliance Among Health Care Staff and Student Nurses in a Mental Health Setting. Issues in Mental Health Nursing, 30:702-704. ISSN 0161-2840 print/ 1096-4673 online. DOI: 10.3109/01612840903079223

PFSense Project (pfSense) (2012). pfSense Open Source Firewall Distribution – Hardware Sizing Guidance. Retrieved on March 15, 2012 from http://www.pfsense.org/index.php?option=com_content&task=view&id=52&Itemid=49

Ray, Ramon (2009, June 8). Using Old Computers Does Not Save you Money. Retrieved on April 01, 2012 from http://smallbiztechnology.com/archive/2009/06/using-old-computers-does-not-s.html/

Recovery.gov (2012). The Recovery Act. Retrieved on March 4, 2012 from http://www.recovery.gov/About/Pages/The_Act.aspx

Red Hat Inc. (Red Hat) (2012). 4.4. Configuration Examples. Retrieved on April 8, 2012 from http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/6/html/Managing_Confined_Services/sect-Managing_Confined_Services-Samba-Configuration_examples.html

Rock, Connie and Stephens, Mike (2008, February). Windows Server 2008 – Planning and Deploying Group Policy. Retrieved on April 8, 2012 from http://www.microsoft.com/download/en/confirmation.aspx?id=22478

Rousskov, Alex (2012). Feature: ICAP (Internet Content Adaption Protocol). Retrieved on April 9, 2012 from http://wiki.squid-cache.org/Features/ICAP

RSA, an EMC Company (RSA) (2012). RSA Data Loss Prevention. Retrieved on March 28, 2012 from http://www.emc.com/security/rsa-data-loss-prevention.htm

Samba.org (2012). What is Samba? Retrieved on April 8, 2012 from http://www.samba.org/samba/what_is_samba.html

Securehq.com (2012). Websense Websense WebSense Security Gateway. Retrieved on April 9, 2012 from http://www.securehq.com/group.wml&groupid=1453

Siemens Corporation (Siemens) (2012). Soarian Integrated Care. Retrieved on April 8, 2012 from http://www.medical.siemens.com/siemens/en_GB/gg_hs_FBAs/files/HIE/SIC_ProductBrochure_e_2006.pdf

Snort.org (2012). About Snort. Retrieved on March 15, 2012 from http://www.snort.org/snort

Snyder, Joel (2012). CSI: Five Critical Questions for NAC. Retrieved on March 8, 2012 from http://www.exclusive-networks.com/downloads/it/documentations/5%20Critical%20questions%20for%20NAC.pdf

Squid-cache.org (2012). Squid: optimizing web delivery. Retrieved on April 9, 2012 from http://www.squid-cache.org/

Stallings, W. (2008) . Computer Security: Principles and Practice. Upper Saddle River, NJ: Pearson Prentice Hall

Stephenson, Peter (2007, November 1). McAfee Data Loss Prevention Appliance. Retrieved on April 9, 2012 from http://www.scmagazine.com/mcafee-data-loss-prevention-appliance/review/1137/

Supremus Group (2012). Covered Entity HIPAA Compliance Tool. Retrieved on March 16, 2012 from http://www.hipaatraining.net/Covered-Entity-HIPAA-Compliance-Tool-less-50employee.htm

Symantec Corporation (Symantec) (2012). PGP Whole Disk Encryption – System Requirements. Retrieved on April 8, 2012 from http://www.symantec.com/products/sysreq.jsp?pcid=pcat_info_risk_comp&pvid=wd_encryption_1

Symantec Corporation (Symantec) (2012). Security and Privacy for Healthcare Providers. Retrieved on March 1, 2012 from http://eval.symantec.com/mktginfo/enterprise/white_papers/b-security_and_privacy_for_healthcare_WP_20934020.en-us.pdf

Symantec Corporation (2012). Symantec Endpoint Encryption Removable Storage Edition. Retrieved on April 8, 2012 from http://www.symantec.com/content/en/us/enterprise/fact_sheets/b-see_removeable_storage_DS_21157418.en-us.pdf

Symantec Corporation (Symantec) (2012). Symantec PGP Whole Disk Encryption – MSRP Per License. Retrieved on April 8, 2012 from http://www.symantec.com/content/en/us/store/volume_pricing/PGP-Whole-Disk-Encryption-081911.pdf

Techotopia.com (2012). Configuring BitLocker Drive Encryption on Windows Server 2003. Retrieved on March 15, 2012 from http://www.techotopia.com/index.php/Configuring_BitLocker_Drive_Encryption_on_Windows_Server_2008

Trend Micro (2012). Worry-free Business Security. Retrieved on March 15, 2012 from http://www.trendmicro.com/cloud-content/us/pdfs/home/brochures/br_worryfree-family.pdf

Touchet BK, Drummond SR, Yates WR: Brief reports: the impact of fear of HIPAA violation on patient care. Psychiatr Serv 2004;55:575–576

Tovino, Stacey A. and Reisz, Cynthia Y. Protecting PHI: Legal Duties of Health Care Lawyers Post-HITECH. Retrieved on April 1, 2012 from http://publish.healthlawyers.org/Events/Programs/Materials/Documents/PHYHHS11/reisz_tovino_including_exhibits_a-b.pdf

TrueCrypt (2012). Frequently Asked Questions. Retrieved on April 8, 2012 from http://www.truecrypt.org/faq

Valdes, I, Kibbe, D.C., Tolleson, G., Kunik, M.E., Petersen, L.A. (2004, February 1). Barriers to Proliferation of Electronic Medical Records. Retrieved on April 1, 2012 from http://www.ingentaconnect.com/content/rmp/ipc/2004/00000012/00000001/art00002#expand/collapse

Venema, Wietse (2012). Postfix TLS Support. Retrieved on March 15, 2012 from http://www.postfix.org/TLS_README.html

Wang, Samuel J., Middleton, Blackford, Prosser, Lisa A., Bardon MD, Christiana G., Spurr, Cynthia D., Carchidi, Patricia J., Kittler, Anne F., Goldszer, Robert C., Fairchild, David G., Sussman, Andrew J., Kuperman, Gilad J., Bates, David W (2003). A cost-benefit analysis of electronic medical records in primary care. The American Journal of medicine, 114(5), 397-403.

Websense Corporation (2012). Websense Web Security: Integrating the Content Gateway component with Third Party Data Loss Prevention Applications. Retrieved on April 9, 2012 from http://www.websense.com/content/support/library/web/v75/wcg_misc/Web_Security_Gateway_DLP_ICAP_Integration.pdf

Whitten, Alma, and Tygar, J.D. (2005). Why Johnny Can't Encrypt – A Usability Evaluation of PGP 5.0. Retrieved on April 8, 2012 from http://www.cs.berkeley.edu/~tygar/papers/Why_Johnny_Cant_Encrypt/OReilly.pdf

WorldVista Inc. (2012). VistA History. Retrieved on March 1, 2012 from http://worldvista.org/AboutVistA/VistA_History

Zandri, Jason (2009, February 19). Windows 7 Editions Comparison. Retrieved on March 28, 2012 from http://www.petri.co.il/windows-7-editions-comparison.htm

Zhivan, Natalia A. and Diana, Mark L. (2012). U.S. Hospital Efficiency and Adoption of Health Information Technology. Health Care Manag Sci (201) 15:37-37 DOI: 10.1007/s10729-011-9179-2

Appendix A- Cloud-based/Remotely Hosted Security Evaluation Matrix

A – Encryption

Control Number	Control	Description	Standard(s)	Applies to Cloud/ Services Provider	Applies to Small/Medium Health Care Organization
A100	Emergency Access	Does the organization permit authorized emergency user access to ePHI during an emergency	**§164.312(a)(2)(ii), §170.302(p)**	Yes	Yes
A101	Encryption of data at remote sites	Does the organization allow for encryption of data so that unauthorized personnel at the remote site do not have access to the data?	**45 CFR 160 and 164, §170.302(u),**	Yes	Yes
A102	Encryption of portable media and hard drives	Does the organization encrypt protected health information at risk of being lost on hard drives or removable media such as USB drives or portable hard drives?	**45 CFR 160 and 164**	Yes	Yes
A103	Device and Media Controls	Does the organization have the ability to track the transfer of ePHI onto electronic media that may be able to be removed from the facility, such as USB drives, laptops, or removable hard drives?	**§164.310(d)(1)**	Yes	Yes

Control Number	**Control**	**Description**	**Standard(s)**	**Applies to Cloud/ Services Provider**	**Applies to Small/Medium Health Care Organization**
A104	Transmission Security	Does the organization encrypt and decrypt data when exchanging electronic health information using approved security functions as defined by Annex A of NIST FIPS 140-2?	**§164.312(e)(1), §170.302(v), 45 CFR 160 and 164, HITSP/T17**	Yes	Yes
A105	Encryption	Does the organization encrypt electronic health information at rest using approved security functions as defined by Annex A of NIST FIPS 140-2?	**§170.302(u), 45 CFR 160 and 164, HITSP/T16**	Yes	Yes
A106	Integrity	Does the organization implement policies, procedures, and technical controls to ensure that protected health information is not altered or destroyed in an unauthorized manner?	**§164.312(c)(1), §170.302(s), HITSP/T15**	Yes	Yes

B – Technical Policy and Unique User Identification/Access Control

Control Number	Control	Description	Standard(s)	Applies to Cloud/ Services Provider	Applies to Small/Medium Health Care Organization
B100	Workstation Logical/Physical Security	Are there physical safeguards to only allow access to ePHI on workstations by authorized users?	**§164.310(c)**	Yes	Yes
B101	Access Control	Does the organization implement policies and procedures for allowing access to those persons or software programs that have been granted access rights?	**§164.312(a)(1)**	Yes	Yes
B102	Unique User Identification	Does the organization assign a unique user name and/or number for tracking user identity when accessing ePHI? Does this extend to system services and/or applications? NOTE: This means that default user accounts or shared accounts cannot be used for accessing ePHI, providing technical support to systems containing it, or running services or shared applications that process it.	**§164.312(a)(2)(i), §170.302(o)**	Yes	Yes

Control Number	Control	Description	Standard(s)	Applies to Cloud/ Services Provider	Applies to Small/Medium Health Care Organization
B103	Audit Controls	Does the organization implement hardware, software, and procedural mechanisms to record and examine activity in systems that contain ePHI?	**§164.312(b), §170.302 (r), HITSP/T15**	Yes	Yes
B104	Person or Entity Authentication	Does the organization implement policies or procedures to verify that a person or entity that wants access to ePHI is who they claim to be?	**§164.312(d), §170.302(t), HITSP/C19**	Yes	Yes
B105	Consistent Time	Does the organization use NTP or SNTP to synchronize time across all computer systems that access PHI?	**HITSP/T16**	Yes	Yes
B106	Non-repudiation/Centralized Authentication	Does the system which contains ePHI use non-repudiation of origin to ensure that whoever enters, changes, or deletes data is who they say they are? I.E. do they use a centralized authentication system, PKI, or similar system such as Active Directory or Kerberos? Do the SSL certificates used provide assertion that the sites are who they say they are?	**HITSP/C26, HITSP/T17, HITSP/T15, HITSP/T16, §164.306(a)(4), §164.308(a)(3)(i)**	Yes	Yes

Control Number	Control	Description	Standard(s)	Applies to Cloud/ Services Provider	Applies to Small/Medium Health Care Organization
B107	Document Updates	Is documentation on systems updated periodically when changes to the environment that affect systems containing protected health information are made?	**§164.316(b)(2)(iii)**	Yes	Yes

C – Proxy Server and Data Loss Prevention

Control Number	Control	Description	Standard(s)	Applies to Cloud/ Services Provider	Applies to Small/Medium Health Care Organization
C100	Transmission Security	Does the organization encrypt and decrypt data when exchanging electronic health information using approved security functions as defined by Annex A of NIST FIPS 140-2?	**§164.312(e)(1), §170.302(v), 45 CFR 160 and 164, HITSP/T17**	Yes	Yes
C101	Protection against unauthorized disclosure	Has the organization implemented controls that protect against any reasonably anticipated disclosures?	**§164.306(a)(3), 45 CFR Parts 160 and 164, §170.210(a)(1), §170.210(a)(2)**	Yes	Yes

Control Number	Control	Description	Standard(s)	Applies to Cloud/ Services Provider	Applies to Small/Medium Health Care Organization
C102	Device and Media Controls	Does the organization have the ability to track the transfer of ePHI onto electronic media that may be able to be removed from the facility, such as USB drives, laptops, or removable hard drives?	**§164.310(d)(1)**	Yes	Yes

D – Firewall

Control Number	Control	Description	Standard(s)	Applies to Cloud/ Services Provider	Applies to Small/Medium Health Care Organization
D100	Protection against unauthorized disclosure	Has the organization implemented controls that protect against any reasonably anticipated disclosures?	**§164.306(a)(3), 45 CFR Parts 160 and 164, §170.210(a)(1), §170.210(a)(2)**	Yes	Yes

Control Number	Control	Description	Standard(s)	Applies to Cloud/ Services Provider	Applies to Small/Medium Health Care Organization
D101	Physical Safeguards	Does the organization implement policies and procedures to limit physical access to its electronic information systems and their physical facilities, while allowing authorized access?	**§164.310(a)(1)**	Yes	Yes
D102	Integrity	Does the organization implement policies, procedures, and technical controls to ensure that protected health information is not altered or destroyed in an unauthorized manner?	**§164.312(c)(1), §170.302(s), HITSP/T15**	Yes	Yes

E – Antivirus

Control Number	Control	Description	Standard(s)	Applies to Cloud/ Services Provider	Applies to Small/Medium Health Care Organization

E100	Integrity	Does the organization implement policies, procedures, and technical controls to ensure that protected health information is not altered or destroyed in an unauthorized manner?	**§164.312(c)(1), §170.302(s), HITSP/T15**	Yes	Yes
E101	Protection against unauthorized disclosure	Has the organization implemented controls that protect against any reasonably anticipated disclosures?	**§164.306(a)(3), 45 CFR Parts 160 and 164, §170.210(a)(1), §170.210(a)(2)**	Yes	Yes

F – Policies, Procedures, Risk/Impact Analysis, and Contracts

Control Number	Control	Description	Standard(s)	Applies to Cloud/ Services Provider	Applies to Small/Medium Health Care Organization
F100	ONC-ATCB Certification	Is the Cloud/Remotely-hosted EMR Solution ONC-ATCB Certified by CCHIT for the current year?	**CCHIT ONC-ATCB Certification Controls**	Yes	
F101	Service Level Agreement	Does the Cloud Services provider have a service level agreement that defines acceptable levels of service interruption, downtime, and notification of adverse events?	**AICPA Service Organization Controls**	Yes	

Control Number	Control	Description	Standard(s)	Applies to Cloud/ Services Provider	Applies to Small/Medium Health Care Organization
F102	Service Organization Controls 2 Report	Does the hosting organization or data center have a Service Organization Controls 2 report that documents the implementation effectiveness of privacy and security controls?	**AICPA Service Organization Controls, §164.306(a)(2), §164.308(a)(ii)(A), 164.308(a)(ii)(B), 164.306(a)(3), 45 CFR Parts 160 and 164, §170.210(a)(1), §170.210(a)(2), §164.306(a)(4), §164.308(a)(3)(i), §164.308(a)(4)(i), §164.308(a)(5)(i), §164.308(a)(ii)(D)**	Yes	Yes, if they are a service provider.
F103	Security Risk Analysis	Has the organization undergone a security risk analysis to determine the most likely threats?	**§164.306(a)(2), §164.308(a)(ii)(A)**	Yes	Yes
F104	Security Risk Mitigation	Has the organization implemented reasonable and appropriate countermeasures to the risks identified in the risk assessment?	**§164.308(a)(ii)(B)**	Yes	Yes
F105	Workforce Security Compliance Standards	Has the organization taken steps to ensure that its workforce complies with HIPAA security standards?	**§164.306(a)(4), §164.308(a)(3)(i)**	Yes	Yes

Control Number	Control	Description	Standard(s)	Applies to Cloud/ Services Provider	Applies to Small/Medium Health Care Organization
F106	Workforce Security	Has the organization implemented policies and procedures to ensure that all workforce members have access to protected health information that require it?	**§164.308(a)(3)(i)**	Yes	Yes
F107	Workforce Sanctions	Has the organization implemented sanctions on workforce members who do not comply with security policies and procedures?	**§164.308(a)(ii)(C)**	Yes	Yes
F108	Information Access Management	Has the organization implemented policies and procedure for authorizing access to protected health information consistent with acceptable usage standards?	**§164.308(a)(4)(i)**	Yes	Yes
F109	Security awareness and training	Has the organization implemented a security awareness and training program for all organization members, including management?	**§164.308(a)(5)(i)**	Yes	Yes
F110	Audit Log Review	Has the organization implemented procedures to review records of information system activity, including audit logs, access reports, and incident tracking reports on a regular basis?	**§164.308(a)(ii)(D)**	Yes	Yes

Control Number	**Control**	**Description**	**Standard(s)**	**Applies to Cloud/ Services Provider**	**Applies to Small/Medium Health Care Organization**
F111	Assigned Security Responsibility	Has a security official who is responsible for the required policies and procedures been identified?	**§164.308(a)(2)**	Yes	Yes
F112	Security Incident Procedures	Has the organization implemented policies and procedures to address security incidents, including response, mitigation, and documentation of incidents and their outcomes?	**§164.308(a)(6)(i)**	Yes	Yes
F113	Contingency Plan	Has the organization established and implemented policies and procedures for responding to emergencies or other unnatural occurrences, including backups, a disaster recovery plan, and an emergency mode operations plan?	**§164.308(a)(7)(i)**	Yes	Yes
F114	Business Impact Analysis	Has the organization performed a Business Impact Analysis to predict the consequences of a disruption in business operations and gather the information required to develop recovery strategies?	**Required by §164.308(a)(7)(i)**	Yes	Yes

Control Number	Control	Description	Standard(s)	Applies to Cloud/ Services Provider	Applies to Small/Medium Health Care Organization
F115	Periodic Evaluation	Does the organization perform periodic technical and non-technical re-evaluations of environmental and operational changes that can affect the security of protected health information?	**§164.308(a)(8)(i)**	Yes	Yes
F116	Business Associates	Does the organization ensure that its business associates that deal with protected health information appropriately protect the data?	**§164.308(b)(1)**	Yes	Yes
F117	Physical Safeguards	Does the organization implement policies and procedures to limit physical access to its electronic information systems and their physical facilities, while allowing authorized access?	**§164.310(a)(1)**	Yes	Yes
F118	Workstation Use	Are their policies and procedures that govern proper workstation usage?	**§164.310(b)**	Yes	Yes
F119	Workstation Physical Security	Are their policies and procedures that govern the physical placement of a workstation and its surroundings to protect ePHI?	**§164.310(b)**	Yes	Yes

Control Number	**Control**	**Description**	**Standard(s)**	**Applies to Cloud/ Services Provider**	**Applies to Small/Medium Health Care Organization**
F120	Device and Media Controls	Does the organization have policies and procedures that govern the receipt and removal of physical or electronic media that contains ePHI into and out of the facility?	**§164.310(d)(1)**	Yes	Yes
F121	Disposal Procedures	Does the organization have policies and procedures governing the final disposition of ePHI, and the hardware and media which may store it?	**§164.310(d)(2)(i), 45 CFR 160 and 164**	Yes	Yes
F122	Media re-use	Does the organization have policies and procedures governing the removal of ePHI from electronic media before it is made available for re-use	**§164.310(d)(2)(ii), 45 CFR 160 and 164**	Yes	Yes
F123	Business Associate Agreements	Do the Business Associate agreements stipulate that business associates will implement the proper administrative, physical, and technical safeguards which will reasonable and appropriately protect the confidentiality, integrity, and availability of protected health information?	**§164.314(a)(1)(i), §164.314(a)(2)(i)(A)**	Yes	Yes
F124	Subcontractors	Do the Business Associate agreements stipulate that subcontractors will also take reasonable and appropriate safeguards to protect ePHI?	**§164.314(a)(2)(i)(B)**	Yes	Yes

Control Number	Control	Description	Standard(s)	Applies to Cloud/ Services Provider	Applies to Small/Medium Health Care Organization
F125	Reporting of incidents	Do the Business Associate agreements require contractors or subcontractors to report any security incidents to the covered entity of which they are aware?	**§164.314(a)(2)(i)(C)**	Yes	Yes
F126	Termination of contract	Do the Business Associate agreements give the right to terminate the contract if the covered entity determines that they are in violation of the contract?	**§164.314(a)(2)(i)(D)**	Yes	Yes
F127	Government Organization	If the covered entity and its business associate are government organizations, is there a memorandum of understanding that stipulates that data will be protected as per the HIPAA Security Rule?	**§164.314(ii)(A)(1)**	Yes	Yes
F128	Good Faith	If a business associate is required by law to collect information and cannot meet security requirements as per the HIPAA Security Rule, it can continue to provide services provided it attempts in good faith to comply	**§164.314(ii)(B)**	Yes	Yes

Control Number	Control	Description	Standard(s)	Applies to Cloud/ Services Provider	Applies to Small/Medium Health Care Organization
F129	Termination Clause Omission	A covered entity may omit the authorization of contract termination if it is in conflict with the statutory obligations of the covered entity or its business associate	**§164.314(ii)(C)**	Yes	Yes
F130	Group Health Plans	If the business associate is a group health plan, and unless the information is used for marketing, plan management, or enrollment status purposes, the plan must appropriately safeguard and protect ePHI	**§164.314(b)(1)**	Yes	Yes
F131	Policies and Procedures	Are organizational policies and procedures maintained in electronic and written form?	**§164.316(a)**	Yes	Yes
F132	Policies and Procedure Implementation	Has the organization implemented reasonable and appropriate policies and procedures to comply with the HIPAA Security Rule?	**§164.316(a)**	Yes	Yes
F133	Documentation	Does the organization maintain written records of assessments, actions, or incidents that occur?	**§164.316(b)(ii)**	Yes	Yes
F134	Anti-overlook policies	Does the organization not permit or excuse actions that violate HIPAA requirements?	**§164.316(a)**	Yes	Yes

Control Number	**Control**	**Description**	**Standard(s)**	**Applies to Cloud/ Services Provider**	**Applies to Small/Medium Health Care Organization**
F135	Document Retention	Does the organization have document retention policies that retain organizational policies, procedures, and documentation for a period of at least six years from creation or last effective date, whichever is later?	**§164.316(b)(2)(i)**	Yes	Yes
F136	Document Updates	Is documentation on systems updated periodically when changes to the environment that affect systems containing protected health information are made?	**§164.316(b)(2)(iii)**	Yes	Yes

Appendix B - Glossary

ACS: Affiliated Computer Services

AD: Active Directory

AICPA: American Institute of Certified Public Accountants

ARRA: American Reinvestment and Recovery Act

BIA: Business Impact Analysis

CCHIT: Certification Commission for Health Information Technology

CIFS: Common Internet File System

CIO: Chief Information Officer

CISO: Chief Information Security Officer

CMS: Center for Medicare and Medicaid Services

CPA: Certified Public Accountant

DLP: Data Loss Prevention

EACH: EHR Alternative Certification for Healthcare providers

EMR: Electronic Medical Record

EHR: Electronic Health Record

ePHI: Electronic Protected Health Information

FIPS: Federal Information Processing Standards

GPO: Government Printing Office

HHS: Department of Health and Human Services

HIPAA: Health Information Portability and Accountability Act

HITECH Act: Health Information Technology for Economic and Clinical Health Act

HITSP: Healthcare Information Technology Standards Panel

ICAP: Internet Content Adaption Protocol

IDS: Intrusion Detection System

IPS: Intrusion Prevention System

NAC: Network Access Control

NIST: National Institute of Standards and Technology

NTP: Network Time Protocol

ONC-ATCB: Office of the National Coordinator – Authorized Testing and Certification Body

PGP: Pretty Good Privacy

PHI: Protected Health Information

SAS: Statement on Auditing Standards

SMB: Server Message Block

SOC: Service Operational Controls

USB: Universal Serial Bus

Temple University

Improving Healthcare Provider Information Security Through the Implementation of Financial Systems Structures and Controls

August 2014

TEMPLE UNIVERSITY

Improving Healthcare Provider Information Security Through the Implementation of Financial Systems Structures and Controls

SGM 5182 Independent Study Project

Parker, Mitchell

8/5/2014

EXECUTIVE SUMMARY

Two of the most critical industries in the United States are finance and healthcare. Finance is responsible for the efficient transferal of monetary value across the world. Healthcare ensures the well-being of the American population. One salient item that both have in common is that both industries are subject to a myriad of regulations and guidance to ensure secure and efficient operations. However, that is where the similarities end. While both have no shortage of checks and balances, finance is much more well-organized and governed.

The purpose of this paper is to illustrate the differences between the approaches to Information Security in finance and healthcare. The centralized model in finance will be explained. The main entity responsible for ensuring security, which is the Center for Medicare and Medicaid Services, will have its role and regulations explained. The issues with the current model in healthcare will be explored in detail. Reasons why this current situation exists will then be explained thoroughly. These reasons will include structural, legal, and situational, and financial analysis of healthcare providers' current state. A SWOT analysis will be used to discuss the current situations with healthcare information security in the context of policies, procedures, and effective communication. Means by which the hospital and healthcare industry can improve this situation will then be explored through the use of a similar enterprise risk management structure as finance, and the use of Healthcare Information Exchanges (HIEs) as a strategic tool. A risk/feasibility analysis of this potential solution and some of its pitfalls will be explored. The overall goal is to demonstrate the application of Information Security controls from the Financial Services community can potentially lead to efficiencies and a reduction of fraud, waste, and abuse with healthcare providers.

CENTRALIZED FINANCE INFORMATION SECURITY MODEL

Applicable financial institutions, under Section 501(b) of the Graham-Leach Bliley Act (GLBA), are required to establish appropriate standards to insure the security and confidentiality of customer records and information, protect against any anticipated threats or hazards to their security and integrity, and to protect against unauthorized access or use that could lead to customer harm (106th Congress, 1999). These aforementioned financial institutions include federally chartered banks, members of the Federal Reserve systems, federal and state branches of international banks, banks insured by the Federal Deposit Insurance Corporation (FDIC), savings associations insured by the FDIC, credit unions insured by the National Credit Union Association, brokers and dealers insured by the Securities and Exchange Commission, investment advisors, and insurance companies (106th Congress, 1999).

The Federal Financial Institutions Examination Council (FFIEC) is a formal interagency body empowered to establish principles, standards, and report forms for the federal examination of financial institutions (FFIEC, 2014). They are given such power by their member agencies, which include the Federal Reserve Board (FRB), Federal Deposit Insurance Corporation (FDIC), the National Credit Union Association (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (FFIEC, 2014). They are also empowered to make recommendations to promote uniformity in the supervision of financial institutions (FFIEC, 2014). In addition, they also provide training for state examiners upon request (FFIEC, 2014). The FFIEC trains and certifies financial examiners using the same training programs across the Financial Services industry (FFIEC, 2014).

As part of these standards, the FFIEC has developed the FFIEC IT Examination HandBook InfoBase (FFIEC, 2014). This handbook provides standards, expectations, and guidance on Audit, Business Continuity, Development and Acquisition, Electronic Banking, Information Security, Management, Operations, Outsourcing Technology and vendor solutions, Retail Payment Systems, Supervision of Technology Service Providers, and Wholesale Payment Systems (FFIEC, 2014). This Infobase is the one playbook used by federal (and many state) auditors and inspectors as a reference platform. Enforcement actions on violations of these standards and guidance in the Infobase are the responsibility of the member agencies (FFIEC, 2014).

According to the FFIEC's IT Handbook Infobase, which is the standard financial services guidance, development of the Information Security Program for applicable financial institutions is the responsibility of organizational management (FFIEC, 2014). The Board of Directors is responsible for approving it (FFIEC, 2014). The Board, according to the Graham-Leach Billey Act, is also responsible for overseeing the development, implementation, and maintenance of the program (FFIEC, 2014). It is also responsible for assigning the specific responsibility for its implementation (FFIEC, 2014). The Board is also responsible for approving the written information security policies and overall program at least annually (FFIEC, 2014). This approach of top-down assignment of responsibility starting with the Board of Directors, certified examiners with a standardized curriculum, communication of requirements to all stakeholders, Homeland Security directives directing organizations to share information, and a large centralized Information Sharing community show a strong approach to Information Security in finance.

The Financial Services Information Sharing and Analysis Center (FS-ISAC) was established in 1999 in response to 1998's Presidential Directive 63, and revised by Homeland Security Presidential Directive 7 (FS-ISAC, 2014). These directives mandated that private and public sector organizations share information about physical and cyber security threats and vulnerabilities (FS-ISAC, 2014). The New York State Department of Financial Services, in their May 2014 Report on Cyber Security in the Banking Sector, recommended that all New York State-chartered depository financial institutions become members of FS-ISAC (NYS DFS, 2014). The reason for this is because the rapid pace of change has made it more critical that these institutions use the information-sharing and analysis resources available to them (NYS DFS, 2014). The Commonwealth of Massachusetts' Division of Banks has issued similar guidance to all of their state-chartered banks on June 18, 2014 (Commonwealth of Massachusetts, 2014). As of 2011, over 4,000 institutions belong to the FS-ISAC (FS-ISAC, 2011). This is the latest membership count available.

Furthermore, this approach to Information Security governance in Finance has led to more developed Enterprise Risk Management programs in this industry (J of Healthcare Risk Mgmt, 2005). Enterprise Risk Management, which provides a global view of risk throughout the organization, requires the support of the board and CEO. Since they are held accountable under GLBA, the maturity of Enterprise Risk Management programs can be seen as a possible outgrowth of it.

HEALTHCARE INFORMATION SECURITY MODEL

The Center for Medicare and Medicaid Services (CMS), under the guidance of their Office for Civil Rights (OCR), requires applicable organizations, known as Covered Entities, to be compliant with the HIPAA Privacy Rule, and the HIPAA Security Rule (CMS, 2014). Covered Entities are health care providers that transmit information electronically in connection with a transaction for which the Department of Health and Human Services has adopted a standard (CMS, 2014). HIPAA does require health plans and health care clearinghouses, which are organizations that process nonstandard transactions and information into standard ones, to comply (CMS, 2014). The transactions include claims and encounter information, payment and remittance advice, claims status, eligibility, enrollment and disenrollment, referrals and authorizations, coordination of benefits, and premium payment (CMS, 2014). This can be widely interpreted to mean that anyone who submits a claim using a standard format, or uses a tool which does so, is subject to the provisions of the HIPAA Privacy Rule and HIPAA Security Rule.

Business Associates, which are third parties that conduct business on behalf of covered entities, are also subject to the provisions of HIPAA. They are required to only use the Protected Health Information for only the intended purposes of the covered entity (CMS, 2014). They are required to safeguard the information, and will assist the covered entity in complying with some of their duties under the HIPAA Privacy Rule (CMS, 2014). In addition, they are required to notify the covered entity in the case of a breach, and are required to remediate it (CMS, 2014). This requires that the covered entity get satisfactory assurances in writing, specifically in the form of a contract or agreement, to ensure this (CMS, 2014).

There are four main rule sets for HIPAA. The first is the HIPAA Privacy Rule, defined as 45 CFR Part 160 and subparts A and E of 45 CFR Part 164 (CMS, 2014). The HIPAA Security Rule is defined as 45

CFR Part 160 and subparts A and C of 45 CFR Part 164 (CMS, 2014). The Breach Notification Rule is defined as 45 CFR Part 164, subparts 400-414 (CMS, 2014). The HITECH Act, which promotes the adoption and meaningful use of health information technology, was adopted in 2009. It establishes four categories of violations and levels of culpability. It also establishes four corresponding penalty tiers, and sets a maximum penalty of $1.5 million for all violations of an identical provision (CMS, 2014).

There is no corresponding training program or set of standards for all covered entities and business associates to follow. These entities are expected to interpret and apply the rules by themselves. In an interview with Dave Snyder, Chief Information Security Leader for Independence Blue Cross, on June 30th, 2014, he indicated that the stances of CMS and the Office of the National Coordinator are to allow the industry to police itself (Snyder, 2014). CMS has not agreed upon a security framework (Snyder, 2014). CMS does provide training for providers on HIPAA in conjunction with Medscape, one of the more popular medical web sites (Medscape, 2014). However, there is no evidence of a comprehensive training program for the HIPAA Privacy Rule, HIPAA Security Rule, Breach Notification Rule, or HITECH Act.

In December of 2013, eHealth Initiative, a non-profit policy and advocacy group based out of Washington DC, held an event called “Integrating Privacy & Security into Organizational Strategy & Culture”. During this event, representatives from both the Office of Civil Rights (OCR) and Office of the National Coordinator (ONC) spoke. The representative from the Office of Civil Rights indicated that there was a need to implement necessary training and education for Business Associates to make them aware of HIPAA rules (eHealthInitiative, 2014). She also stated that healthcare organizations are ultimately responsible for making their business associates aware of their privacy and security obligations (eHealthInitiative, 2014). Advisory Board participants indicated that the HIPAA Security Rule as challenging and in need of clarity (eHealth Initiative, 2014).

The current model in healthcare is to provide the regulations with little corresponding training. There is little clarity being given to the HIPAA Security Rule, which is causing consternation with a large group of providers. Representatives of the Mayo Clinic, Children's Hospital of Philadelphia, PriceWaterhouseCoopers, HITRUST, United Healthcare, Cooper Health, and Merck were present at this meeting (eHealth Initiative, 2014). These entities all expressed difficulty with complying with rules in need of clarity.

The HIPAA Security Rule requires that organizations train their workforces on the Information Security Rule (AHIMA, 2014). The American Health Information Management Association, AHIMA, developed a training guide which covers the organizational requirements for training. They indicate that as part of the HITECH Act, CMS has made an individual available in each regional HHS office to provide training and education about everyone's rights and responsibilities under the HIPAA Privacy and Security rules (AHIMA, 2014). There are 10 regional offices for the entire United States. This means that there are 10 people that provide this training for tens of thousands of affected providers.

Unlike the financial industry, there is no guidance given on implementation. CMS published their internal 2010 System Security Procedure, which is available from their web site (CMS, 2010). Their own security plan gives ultimate authority for Information Security to the Chief Information Officer, not the Chief Information Security Officer (CMS, 2010). They also make security training the responsibility of the business owner in their Roles & Responsibilities Matrix (CMS, 2010). This is a disjointed structure that can lead to wildly differing communication about security responsibilities due to no centralized Information Security training resources. The Business Owner does not have the requisite training in Information Security, and the CISO does in their matrix (CMS, 2010).

The disjoint approach in Information Security given by CMS' own Information Security plan corresponds with their current approaches with training outside agencies. The rules and regulations are there to follow, but there is little, if any, centralized security guidance given to customers, be they internal or external.

ISSUES WITH HEALTHCARE MODEL

There are three major parts of the commerce system. There are the financial services providers, such as banks and lenders. There are the producers of goods and services that customers utilize. Finally, there are the consumers of both financial services and the producers of goods and services. Out of these three, only one of them has tight Information Security regulations, financial services. Only Financial Services has a comprehensive monitoring program enforced by government regulatory standards.

While there are Payment Card Industry (PCI) Information Security Standards for merchants that process credit cards, those controls only apply to the environments that handle them (PCI SSC, 2013). The latest PCI 3.0 standard does emphasize continual monitoring and a robust computing infrastructure, but does not require it for the entire computing environment (PCI SSC, 2013).

According to the National Institute of Standards and Technology (NIST), Information Security can be defined as the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability (Kissel, 2013). The definition of fraud, from the Association of Certified Fraud Examiners, is that it can encompass any crime for gain that uses deception as its principal modus operandus (ACFE, 2014).

Health care fraud, according to the Wex legal dictionary, is a type of white-collar crime that involves the filing of dishonest health care claims in order to turn a profit (Wex, 2014). It can involve the providing of false information, misuse of legitimate information, billing for unneeded services, or altering of medical information (Wex, 2014). Information security is relevant to health care fraud because Information Security involves the protection of information and information systems from misuse. Health care fraud is a misuse of legitimate information and information systems to commit crime. The issue present is that there is a significant amount of health care fraud, and that the current enforcement mechanisms as they relate to information security are not capable of dealing with the situation.

Estimates of the cost of health care fraud vary wildly. The aforementioned Wex legal dictionary estimates that 10 cents of every dollar spent on health care goes toward paying for fraudulent health care claims (Wex, 2014). Berwick and Hackbarth, in their paper Eliminating Waste in US Health Care, estimated that fraud and abuse accounted for between $82 billion and $272 billion in wasteful spending in 2011 (Berwick and Hackbarth, 2012). The Association of Certified Fraud Examiners (ACFE) indicated that 6.7% of reported fraud claims came from health care. T.R. Goldman, in the policy brief Eliminating Fraud and Abuse, from the journal Health Affairs, had several different figures. The first, from CMS themselves, indicated that Medicare and Medicaid made $65 billion in improper federal payments in fiscal year 2010 (Goldman, 2012). When improper payments made by states were included, that raised the total by $10 billion (Goldman, 2012). His interpretation of the Berwick and Hackbarth study estimated that fraud and abuse contributed as much as $98 billion to Medicare and Medicaid spending in 2011 (Goldman, 2012). For the purposes of this paper, the estimation of fraud will be between $75 to $98 billion dollars yearly.

In 2012, Healthcare and related services had a 17.2% share of the US Gross Domestic Product (GDP) (Lassman et al., 2014). That is $2.8 trillion dollars in spending on healthcare in the United States in 2012. Financial Services and Insurance companies, according to the US Department of Commerce, had a 7.9% share of US GDP, with an estimated spend of $1.24 trillion dollars in financial services.

The 2013 LexisNexis True Cost of Fraud Study indicated that retailers had lost an estimated 0.54% of revenue to fraud (LexisNexis, 2013). Kroll Advisory Solutions, in the Global Advisory Report, Annual Edition 2012/13, indicated that the average revenue loss from fraud was 1.1% (Kroll Advisory

Solutions, 2013). The estimation of fraud in health care is between 2.68% and 3.5% of overall spending estimating $75 to $98 billion dollars of fraud and $2.8 trillion of overall spending.

This is a significantly higher amount of fraud, by percentage, than the average. Information from health care systems, and the systems themselves, are being misused to commit fraud at a significantly higher rate than the national average. Due to the system and information misuse, this can be construed as both Information Security and Fraud issues.

HIPAA has two major components related to fraud mitigation. The first is that the HIPAA act itself established and funded a program to combat fraud and abuse committed against all health plans, both public and private (USDOJ, 2014). The second is that the HIPAA Security Rule, 45CFR § 164.308 (a)(ii)(D), requires an Information System Activity Review (CMS, 2014). Covered Entities are required to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports (CMS, 2014).

The HITECH Act, in addition, provides financial incentives for organizations to adopt Electronic Medical Record (EMR) technology under the Meaningful Use program (CMS, 2014). This means that providers and hospitals who adopt this technology, which means that they have full electronic records and data sets, can get incentive money back from CMS for demonstrating effective use in their environment.

The Patient Privacy and Affordable Care Act (PPACA), more colloquially referred to as "Obamacare", Public Law 111-148, March 23, 2010, has several more provisions to detect and combat against fraud. Section 6401 calls for enhanced provider screening, including licensing checks, criminal background checks, unscheduled and unannounced site visits, and any other screening deemed appropriate (111th Congress, 2010). Section 6401 also requires organizations to disclose any direct or indirect affiliations with providers that may have been previously sanctioned (111th Congress, 2010).

They have the right to deny enrollment to any organization that poses an undue risk of fraud, waste, or abuse (111th Congress, 2010).

Section 6401 also allows CMS to adjust payments of providers of services and suppliers for past due obligations (111th Congress, 2010). This means that any organization that has outstanding obligations to CMS will just have them taken out of receivables. This also means that providers, who typically run very low profit margins, run the risk of losing revenue instead of negotiating a payment plan with CMS. Section 6401(a)(3) of the PPACA also establishes the requirement that providers and suppliers have a compliance program in place (111th Congress, 2010).

Section 6402, the Enhanced Medicare and Medicaid Program Integrity Provisions, amends Part A of title XI of the Social Security Act (42 USC 1301) to add a new section, 1128J, which establishes, at a minimum, a data repository for all claims submitted to Medicare and Medicaid (Title XVIII and XIX), State Children's Health Insurance (Title XXI), Health-related programs from the Veterans' Administration, Department of Defense, Federal old-age and survivors insurance trust fund and federal disability insurance trust fund (Title II), and Indian Health Service data (111th Congress, 2010). Medicare and Medicaid data has priority for inclusion (111th Congress, 2010). The purpose of this is to collect data for fraud, waste, and abuse (111th Congress, 2010). This also gives the Attorney General full access to said claims data for the purpose of examining it for fraud, waste, and abuse (111th Congress, 2010).

Section 6407 requires a face to face encounter with a patient before certifying eligibility for home health services or durable medical equipment under the Medicare program (111th Congress, 2010). This was put in to guard against people abusing this program to sell unnecessary equipment to patients that may not need it. Section 6504 requires providers to report an expanded set of data elements to detect fraud and abuse (111th Congress, 2010).

The provisions within PPACA have good intentions. However, there are several factors which preclude their adoption in a way that benefit hospitals. These options will be looked at to show how economic factors and other initiatives such as ICD-10, Meaningful Use, HCAHPS (Patient Satisfaction), and Recovery Audit Contractor (RAC) audits may impact the ability of organizations to comply with the anti-fraud stipulations in HIPAA, HITECH, and PPACA.

First of all, hospitals are low-margin businesses. According to the American Hospital Association, in a survey of member community hospitals by Avalere Health of 2012 economic data, the average total hospital margin is 7.8% (AHA, 2014). 21.3% of surveyed hospitals have negative total margins (AHA, 2014). 25.9% of surveyed hospitals have negative operating margins (AHA, 2014). The percentage change of the Employment Cost Index for hospitals is 2.8% (AHA, 2014).

According to the 2013 edition of AHA Hospital Statistics, out of the nearly 5,000 nonfederal, short-term general community hospitals in the United States, the average revenue is $151.9 million, and the average profit per hospital is $10.7 million (Herman, 2013). This indicates an average profit margin of 7.04%. One other item of note is that the median average age of plant in 2012 is 10.2 years, which is up from 8.2 in 1992 (AHA, 2013).

The cost of ICD-10 implementation, which is the International Code of Diseases, Version 10, requires providers to implement new codes for billing. According to a cost study initiated by the American Medical Association and conducted by Nachimson Advisors, it will cost between $2 and $8 million dollars to implement ICD-10 in a large physician practice (AMA, 2014). This is a significant cost for practices to bear, and the study includes the loss of productivity and payment disruption in it (AMA, 2014). In addition, the AMA notes that claims denial rates could increase 100 to 200 percent in the initial stages of ICD-10 adoption (AMA, 2014). This is a major financial risk for hospitals that has long-reaching implications.

Adoption of Electronic Medical Records, which is required for Meaningful Use, has several high costs as well. An analysis by Dr. RJ Teufel of the Medical University of South Carolina in the Journal of Academic Pediatrics in 2012 analyzed 4,605,454 weighted discharges by hospitals (Acad Pediatr., 2012). The analysis indicated that EMR was associated with a 7% average greater cost per case (Acad Pediatr., 2012). In addition, hospitals that do not adopt and demonstrate meaningful usage of EMR systems will only receive 75 percent of the adjustment to their Inpatient Prospective Payment System reimbursements in year 1 (CMS, 2014). In year 2, they will receive 50 percent, and year 3 onward, only 25 percent of the increases (CMS, 2014).

Meaningful Use incentive payments only cover 20 to 25 percent of the overall implementation costs required to meet the requirements (Sinno, Gandhi, and Gamble, 2011). This is because there are multiple costs to replace ancillary systems that provide a complete picture of care (Sinno, Gandhi, and Gamble, 2011). Sinno, Gandhi, and Gamble also indicate that the cost of implementing an EMR and the required initiatives competes with the limited capital dollars needed for strategic facility decisions, purchase of biomedical equipment, and ancillary clinical systems (Sinno, Gandhi, and Gamble, 2011). Sinno, Gandhi, and Gamble also cite a short-term artificial increase in labor costs due to the demand for skilled clinical analysts exceeding supply (Sinno, Gandhi, and Gamble, 2011).

To protect the Meaningful Use money, hospitals are required to conduct a security risk analysis and implement updates during each reporting period (CMS, 2014). The penalties for not doing so including returning part or all of the Meaningful Use money received (CMS, 2014). Under PPACA, CMS can just take the money out of future receivables (111th Congress, 2010). The 2014 AHA Chartbook, for their set of data, indicated that Medicare accounted for 39.7% of costs by payer type for community hospitals (AHA, 2014). A sudden deduction of margins would cause many hospitals in that data set to have a serious financial event. A risk analysis from a CPA firm such as PriceWaterhouseCoopers can cost over $100,000 per year. Hospitals need to reassign or hire skilled security staff to ensure that the security requirements are met. Even if Meaningful Use is met, the costs of doing so offset the anticipated benefit.

The Hospital Consumer Assessment of Healthcare Providers and Systems (HCAHPS) is a program that surveys patients based on patient satisfaction (Clark, 2012). Hospitals that score poorly on HCAPS surveys can be expected to be penalized 0.4% to 1% on their Medicare payments (Clark, 2012). This potential reduction in revenue may cause hospitals to redirect their focus onto patient satisfaction, since there is a potential loss of revenue there.

In 2005, CMS started a program called the Recovery Audit Program. Third-party Recovery Audit Contractors (RAC) review claims with supporting documentation (CMS, 2014). They determine whether or not the services were necessary, and can issue denials of claims (CMS, 2014). These contractors receive commissions based on the amount of money recovered for Medicare (CMS, 2014). They only can review the past three years of claims (CMS, 2014). They can also audit up to 400 records in a 45-day period (CMS, 2012). Handling this number of audits can cause an extra administrative burden for providers. The Philadelphia Inquirer, in their July 27, 2014 edition, profiled Fox Rehab, a Philadelphia-area company that had to lay off 62 office workers and has had a 15 percent cut in their Medicare reimbursements for outpatient physical therapy (Brubaker, 2014). The American Hospital Association has also weighed in and determined that the RAC program causes urgent and critical problems with additional resources being required to appeal claims (AHA, 2014). They also note that the RAC system is so overloaded that it takes two years to see an administrative law judge (AHA, 2014). The RAC program in itself, while a good idea, causes providers significant overhead and negatively affects their ability to focus on providing care.

There are several other costs to consider as well. Accurately checking the data for fraud and breaches of privacy requires staff and a lot of analysis. In an interview with MedCityNews, Dr. Bimal Desai, the Chief Medical Information Officer for Children's Hospital of Philadelphia, indicated several important facts. He gave an example of how many rows of audit data needed to be reviewed for a patient. For an inpatient with a two week hospital stay, there were over 100,000 rows of data (Baum, 2014). Random audits of 100 patient medical records at other hospitals, in his experience, take one to two full-time employees two weeks (Baum, 2014). He further indicates a large disconnect between what hospitals must do, and what they can actually do (Baum, 2014). Additionally, he indicates that the access logs of EMRs were never designed to detect breaches (Baum, 2014).

The American Hospital Association, in their 2012 AHA Annual Survey, indicates that there were 5,723 registered hospitals in the US (AHA, 2014). There were 36,156,245 admissions to these hospitals in 2012 (AHA, 2014). This averages out to approximately 6,318 admissions per year per hospital. To be able to examine the set of medical records to a 95% confidence level with a 5% confidence interval would require sampling at least 363 records. To be able to examine the set of medical records to a 99% confidence level with a 5% confidence interval would require sampling at least 603 records. If an average hospital examines 1,200 records per year, they are examining their records to at least a 99% confidence level with a 5% confidence interval.

However, dedicating at least two employees to this task would cost approximately $200,000 a year for an average hospital, and significantly more for a much larger facility. Automated tools such as FairWarning may be required for large multi-hospital environments that have complex data integration. Reporting may need to be built in, costing a hospital significantly more money.

With all these additional costs, there is no guidance given on how to implement these systems. What is being done now is a "best guess" estimate given the rules. Information Security and Fraud

Protection is not a fiscal priority for hospitals. Evidence shows that the impact of ICD-10, Meaningful Use, HCAHPS, RAC Audits, and ongoing risk assessments and monitoring are the priorities for keeping hospitals fiscally sound. The AHA's survey also showed the average age of physical plant equipment increasing over the past 20 years, which also shows a potential trend of spending less there to make up for other revenue shortfalls. Since Medicare is a 34.9% chunk of revenue for hospitals in the AHA sample set, affecting that revenue stream may have detrimental effects when the average profit margin of a hospital is 7%. Many hospitals simply do not have the revenue stream to effectively implement Information Security programs to the satisfaction of all of the proscribed government regulations due to competition with other priorities.

HIPAA and HITECH are currently being enforced by direct reporting to the Office of Civil Rights, voluntary reporting, or by compliance reviews (CMS, 2014) (CMS, 2014). CMS has admitted that the HIPAA Security Rule is in need of clarity (eHealth Initiative, 2014). They have also put the onus on training of business associates on the providers themselves (eHealth Initiative, 2014). This has led to a situation where organizations are not even clear on what the requirements are, or what they need to comply to. In this situation, organizations will do the minimum necessary work.

To be able to accurately match patients across multiple organizations, and to be able to use those data sets to prevent fraud, there needs to be a universal identifier. However, in 1998, political and privacy concerns caused Congress to enact legislation as part of the Omnibus Appropriations Act that prevents the Department of Health and Human Services from doing so (AHIMA, 2011). Section 6402 of PPACA establishes a data warehouse for collecting data on all claims to examine them for fraud, waste, and abuse. Medicare and Medicaid still use the Social Security Number for claims (AHIMA, 2011). The act of establishing a data warehouse with all Medicare and Medicaid claims is a potential security risk because the Social Security Number can be used for fraud. Aggregating that data together across multiple providers and entities at a national level provides significant risk. Adding to this, CMS will have the ability to examine all claims from an organization. Even if an organization has examined their medical records to a 99% confidence level, there runs the risk of them detecting fraud or misuse that a well-designed monitoring process may not.

Adding to this, the Office of the National Coordinator has not issued guidelines on patient matching identification yet (eHealth Initiative, 2014). Patient matching is still performed in silos, which leads to privacy risks when payors and providers exchange information (eHealth Intiative, 2014). ONC's Patient Matching Initiative is still in formative discussion stages (Stevens and Black, 2014). This is an outstanding risk in that CMS does not even have the current capability to implement a data warehouse and match patients accurately, and is collecting claims data for one.

The current issues with the healthcare model are that there is a lot of policy in effect, but no centralized guidance and education on it. There is also little clarity on the HIPAA Security Rule. Both HITECH and PPACA add additional checks and balances on top. However, there are provisions of both that cannot be accurately enforced. Due to the lack of clarity, healthcare Information Security is not centrally organized or well-organized, as opposed to the centralized governance model in Financial Services. The current economic situation of hospitals implementing ICD-10, Meaningful Use, Electronic Medical Records, RAC audit programs, and HCACPS with a lower or negative operating margin also leads to less than optimal enforcement of the rules and organizations doing the minimum necessary work. Fraud detection, while mandated as part of PPACA, presents a privacy risk in itself because there is no national healthcare identifier. In addition, the matching algorithms to match patients across organizations accurately have not been vetted yet, meaning that CMS is not even capable of realizing the benefits.

While there is a significant amount of fraud, the low operating margins, resource-intensive RAC audits, HCAHPS, emphasis on changing medical billing and coding via ICD-10, Meaningful Use, and Electronic Medical Records effectively stretch provider resources to the point where fraud detection is not feasible and may cause more economic harm than good. The provider resource issues caused by the RAC program to recover $9 billion show that CMS is not working well with them to resolve fraud and information security issues.

SWOT Analysis of Healthcare Provider Information Security

After describing the issues with Information Security in healthcare, a SWOT analysis of the current situation for these programs providers needs to be performed. This illustrates where resources need to be focused and strategic alternatives developed to help resolve the current situation.

Strengths: 1. Organizations have to comply with HIPAA. 2. Meaningful Use payments require Information Security risk assessments.	Weaknesses: 1. The HIPAA Security Rule is unclear. 2. HITECH Act record review requirements constrain resources.
Opportunities: 1. Resource constraints will cause organizations to think strategically to save money. 2. Health Information Exchanges (HIE), which require interoperability between organizations, are required as part of Stage II Meaningful Use (HealthIT, 2014). 3. Proper organizational alignment will allow Information Security to have more opportunities for influence and action.	Threats: 1. RAC Audits have caused significant resource constraints. 2. ICD-10 implementation has caused resource scarcity. 3. Electronic Medical Records and the corresponding labor cost cause further resource scarcity. 4. Ancillary systems to support EMR cause resource constraints. 5. Aging hospital physical plant requires attention. 6. Section 6401 of PPACA allows Medicare to deduct penalties from receivables. 7. Section 6402 allows CMS to build a data warehouse of all claims to mine for auditing purposes. 8. CMS has not effectively communicated security requirements. 9. CMS is attempting to enforce policies that do not have a sound technical backing (Section 6402 of PPACA). 10. No national identifier for patients, which makes matching more difficult. 11. No proven patient matching algorithms in use by CMS. 12. CMS does have an effective structure for Information Security management.

STRATEGIC ALIGNMENT OF RISK MANAGEMENT

Healthcare providers face multiple external threats to their organization. Fraud, ambiguity and uncertainty on the part of CMS, multiple competing initiatives such as ICD-10 and Meaningful Use, and RAC audits all present clear and present threats to the net income of an organization. There are several ways by which healthcare organizations can strategically realign themselves to resolve these issues. The purpose of these realignments is to realign the organization to better handle ambiguity and uncertainty. Since there is no guidance given on organizational structure, audits, or organizational form like in Financial Services, the ambiguity and uncertainty is magnified.

To provide alignment of resources, the organizational components that handle compliance, privacy, fraud detection, Information Security, Risk Management, and Regulatory Affairs need to report under Enterprise Risk Management. One of the major issues, as Vincent Oliva posited for the insurance industry, was as that industry faced ever-growing regulatory challenges, companies needed to develop an enterprise risk management strategy as information was kept in silos (Oliva, 2007). Generally, in healthcare, Compliance and Privacy report to the Legal department. Information Security usually reports to the Chief Information Officer (Otisik, 2011). Regulatory Affairs usually reports to the Chief Medical Officer. Fraud Detection falls to either Information Security or Compliance. These are all silos separated by executives that do not have dealing with risk as their primary goal.

In this posited new structure, these departments would report to a Chief Risk Officer. The purpose of the Chief Risk Officer is to provide a C-level view of Enterprise Risk Management and a global perspective of the interrelationship of all risks in the organization (J of Healthcare Risk Mgmt, 2005). A 2011 survey of 400 companies found that 79 percent of banks had an enterprise risk management system, as opposed to 67 percent of all companies surveyed (Crosman, 2011). This may be due directly to GLBA legislation and FFIEC/member agency enforcement of it. The Chief Risk Officer would report to both the Board of Directors and the CEO. Having the CRO report to them brings a strategic view of organizational risk to decisions with great gravity.

With the advent of Electronic Medical Records, the operations of the healthcare provider are captured in sophisticated computer systems, in addition to their human capital. This means that the above parties are now involved in a technology-heavy organization, and need to use these EMR systems as an integral part of their jobs. With the numerous external threats caused by RAC Audits, multiple system implementations driven by incentives and regulation, PPACA, and capital requirements, there cannot be silos anymore. Integrating these groups together means that a more flexible organization can respond to issues. As organizations become more reliant upon EMRs, their visibility and risk grows. Decisions on configuration and workflow changes in EMRs now resonate across the organization. An organization that can appropriately assess, plan, and mitigate risk in these systems need to be able to negotiate across it effectively both at the C-level and operationally.

An example of this is in fraud management. Instead of having multiple departments working toward separate solutions for fraud management, Information Security, Risk Management, Compliance, and Privacy could work together toward an integrated solution to address enterprise risk. The same resources that work on RAC audits could be utilized to proactively analyze claims to identify “at risk” claims and address any potential issues. This same team could also work on access reviews and potential pitfalls.

Separating out Information Security from the CIO and moving it under Enterprise Risk Management provides additional checks and balances for critical information systems projects such as ICD-10 and EMRs. Healthcare organizations are required to conduct risk assessments as part of Meaningful Use. Having a separate team consisting of Information Security, Compliance, Privacy, and

Regulatory Affairs under the CRO conducting the risk assessments would remove any conflicts on the part of the CIO, and give an impartial view of the risks to the CEO and Board. As information systems become more critical to the survival of healthcare providers, the need for an enterprise risk management approach to gauge and measure risk becomes prevalent.

Due to a lack of scarce skilled resources, a high degree of ambiguity and uncertainty, and a growing dependence on technology, Enterprise Risk Management should be the governing structure for Information Security, Compliance, and Regulatory initiatives. There needs to be management of risk across the enterprise, and the removal of “silos” of information.

HEALTH INFORMATION EXCHANGE STRATEGY

Health Information Exchanges (HIEs), which are a requirement of Stage 2 Meaningful Use, are a method (and exchange) by which healthcare providers can access and share patient information with each other (HealthIT.gov, 2014). This allows providers to access information from each other without having to directly interface systems. While some HIEs have had significant financial issues, and many have closed (Beck and Wilde Mathews, 2014), there are still significant benefits to be had through integration. The integration from HIEs can parallel the advantages used by information sharing in the Financial Services Information Sharing and Analysis Center (FS-ISAC).

On August 4th, 2014, two of the largest insurers in the state of California, WellPoint and Anthem Blue Cross announced plans to fund the California Integrated Data Exchange, or Cal Index (Beck and Wilde Mathews, 2014). This HIE will contain data on over 9 million patients. Both of these companies are investing in initiatives that tie health provider reimbursements to quality and efficiency methods (Beck and Wilde Mathews, 2014). Having the full patient records available will allow providers to potentially cut out waste and reduce duplication (Beck and Wilde Mathews, 2014). It will also allow providers to see the whole picture when it comes to patients. Since the payors and providers are involved, and there is financial gain to be had through reimbursements, organizations are more likely to participate.

One of the largest problems with HIEs is matching patients across organizations. This takes dedicated resources, as CMS has not figured out how to algorithmically match patients yet (eHealth Initiative, 2014). Utilizing regional HIEs that have payors and providers participating can provide a much smaller data set which can be more easily matched. Patients who have their records transferred and matched via HIE can be flagged by Enterprise Risk Management for audit review. The issues discovered in the audit review process can be utilized to provide better patient matching and continual improvement.

HIEs can also be used to run fraud-detection algorithms on a very large data set. This will allow them to detect fraud patterns across a region that would not be detectable in one provider, such as patients that utilize multiple providers and pharmacies to purchase painkillers. It would also be able to detect multiple orders of durable medical equipment, unnecessary multiple treatments, and excessive orders. Potential fraudulent patients can be flagged using these algorithms as well.

Accountable Care Organizations are groups of doctors, hospitals, and other providers that come together voluntarily to give highly coordinated care to patients (CMS, 2014). The goal of this coordination of care is to make sure that patients get the right care they need, without unnecessary duplication of services and with the prevention of errors (CMS, 2014). HIEs provide a vehicle for all the participants in an ACO to coordinate together to provide a higher standard of care and have one place to look for all of a patient's data. This shared savings model can present incentive for ACOs to participate.

The issue of free riding in HIEs can be mitigated by several factors. First, as Beck and Wilde Mathews indicated, by providing reimbursements based on quality and efficiency to providers for using the HIE to cut out waste and duplication. Secondly, by providing the ability to mine HIE data for fraud, regional patterns of fraud can be detected and potentially remediated. Third, Accountable Care Organizations presents an opportunity for multiple providers and hospitals to integrate data sets and financially benefit from information sharing. Fourth, by keeping the HIE at a regional level, a degree of Clan Control can be achieved, which is a use of social characteristics, such as shared values, commitment, traditions, and beliefs to control behavior (Daft, 2007). Clan Control is critical when ambiguity and uncertainty are high (Daft, 2007). Fifth, there is the potential for establishing HIE-level identities for patients that do not use the Social Security Number. While there is no funding for a national-level patient identifier due to the Omnibus Rule, there is no such specification at the regional level. This can allow providers, once a patient is matched, to carry the identity across multiples. This can also benefit ACOs by allowing them to use that identity in the care process, and more easily identify their patients. This can lead to further efficiencies, both financial and in quality of care.

Information Security can also be better achieved in HIEs by establishing clear standards for data security for participants. By enforcing continual verified security as a condition of participation, the shared risk of data sharing can be mitigated. This can also allow for organizations to share information on how to better secure systems for the purpose of data interchange. Information Security information sharing can be facilitated through HIEs in conjunction with other ISACs, Infragard, the Department of Homeland Security, and other federal and regional agencies.

HIEs, when used properly, can mitigate fraud, provide efficiencies in care, and provide financial benefit. When used at the regional level, they can be used to improve the quality of care within that region. When used with ACOs, they are a necessary tool to properly share information and gain efficiencies. With PPACA, CMS will be establishing their own data warehouse of claims. However, due to the lack of a good matching process, this is not going to happen yet. In the words of Jennifer Covich Bordenick, CEO of eHealth Initiative, in the August 5th, 2014 edition of the Wall Street Journal, “It’s up to the private sector to step in and take over where the federal government left off” (Beck and Wilde Mathews, 2014). It’s to the advantage of providers and payors to reduce fraud, waste, and abuse on their own and develop efficiencies to deal with RAC audits and the eventual data mining that will occur. The current situation with CMS not even having an organizational structure conducive to Information Security only exacerbates the situation.

RISK ANALYSIS

Information Security and Fraud in healthcare is a prevalent issue. These issues stem from a systemic lack of control across healthcare. There is significant risk no matter what decision is made due to the volatility and uncertainty of the environment. The risks of not implementing the strategic recommendations will therefore be discussed.

The risk of not implementing an Enterprise Risk Management program to manage risk across the organization means that healthcare organizations will not be able to structure themselves like the financial community, and will not be able to effectively manage and communicate risk throughout the organization. In addition, the board and CEO will not be held accountable for risk. This also means that the efficiencies gained by centralizing the silos in the organization that manage risk will not be realized. Organizations will not be able to manage fraud, waste, and abuse as efficiently, and the current situation will continue to exist.

The risk of not implementing a Healthcare Information Exchange (HIE) strategy means that providers will be missing opportunities to reduce fraud, waste, and abuse through information sharing and analysis. There will also be missed opportunities for financial enrichment through participation in Accountable Care Organizations. Finally, the organization will not be able to meet criteria for Meaningful Use, meaning that potential revenue loss from the incentive money for implementing an Electronic Medical Record system will occur.

Due to the uncertain structure and implementation of security controls by CMS, including RAC audits, lack of clarity on the HIPAA Security Rule, and the complexity of compliance, strategic actions need to be taken to ensure that healthcare provider organizations are able to adequately identify, prioritize, and manage risk. The current situation, as-is, will lead to a continuation of the status quo. CMS is not structured or able to manage their risk, as evidenced by the enmity and resource drain caused by the RAC program. The structure and organization in their own Security Plan also indicates an organization that does not train its own workforce well, and does not have good communication. Providers need to manage their own risk at an enterprise level, and utilize regional-level resources to assist in doing so due to these factors.

CONCLUSION

Financial Services provides an excellent structural model for ensuring accountability. Their model of centralized policy development and education has led to a simple, centralized model governed by the FFIEC which trains the industry how to identify, prioritize, and manage Information Security risks. This has led to a lower occurrence of fraud in the Financial Services industry. Their model holds the board of directors and management accountable for the establishment, monitoring, and governance of an Information Security Program.

Healthcare, however, is not as organized. There are multiple policies and procedures governing Information Security, specifically the HIPAA Security Rule, HITECH, and PPACA ("Obamacare") . By the admission of their own staff, they have not done a credible job in communication of them to their customers. Their own internal Security Plan and communications also have poor structure and do not provide for the CISO to run a training or communication program, pushing the responsibility on the business owners.

The Medicare program, in particular, suffers from an estimated $75 to $98 billion dollars a year in fraud, waste, and abuse. However, the main recipients of the benefits of this program, hospitals, average 7 percent profit margins. CMS, as part of HIPAA, HITECH, and PPACA, has placed stringent anti-fraud controls on providers. In addition to these controls, they have asked for several high-price and high-resource commitments from organizations in exchange for continued payments, including ICD-10, Meaningful Use, Electronic Medical Records, HCAHPS, and compliance with Recovery Audit Contractor audits. These initiatives compete with Information Security and reducing fraud, waste, and abuse. There is an impact to the bottom line, and the required level of security may not be achievable given limited resources.

What healthcare providers need to bring improvement to their environments and achieve benefits while reducing fraud, waste, and abuse are two key items. First, healthcare providers need to adopt Enterprise Risk Management like many Financial companies have, and unify the resources responsible for it in Risk Management, Information Security, Compliance, Privacy, and Regulatory Affairs into one central organization headed by a Chief Risk Officer that identifies, prioritizes, and manages risk at an enterprise level. This enterprise risk organization would also achieve economies of scale by sharing formerly disparate resources across one Risk organization.

Secondly, providers need to look at Healthcare Information Exchanges as something more than just a requirement for Meaningful Use. There are several opportunities to reduce duplication of tests, enter into incentive programs with payors, and use regional HIEs as a platform for managing ACOs. There are also additional chances to use anti-fraud algorithms against a larger data set to detect potential fraud, waste, and abuse. There are also opportunities to use HIEs to establish regional-level identities for patients, thereby improving patient matching at the grassroots level. They can also replicate the Financial Services Information Sharing and Analysis Center (FS-ISAC) structure at a regional level and improve Information Security communication across healthcare.

There is room for improvement in healthcare provider Information Security. However, due to the uncertain internal and external communication and enforcement of the rules by CMS, it is incumbent upon the providers to improve their own internal risk management structures to more efficiently manage risk internally. It is also incumbent for providers, payors, and ACOs to work together to mitigate shared risks and reduce fraud, waste, and abuse on their own, without waiting for CMS to do so.

REFERENCES

106th Congress (1999, November 12). Public Law 106-102-Nov. 12, 1999. Graham-Leach Bliley Act. Retrieved from http://www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf on August 2, 2014.

111th Congress (2010, March 23). Public Law 111-148-March 23, 2010. The Patient Protection and Affordable Care Act. Retrieved from http://www.gpo.gov/fdsys/pkg/PLAW-111publ148/pdf/PLAW-111publ148.pdf on August 2, 2014.

Acad Pediatr. 2012 Sep-Oct;12(5):429-35. Hospital electronic medical record use and cost of inpatient pediatric care. doi: 10.1016/j.acap.2012.06.004. Epub 2012 Jul 21.

AHIMA. "Limiting the Use of the Social Security Number in Healthcare." *Journal of AHIMA* 82, no.6 (June 2011): 52-56.

American Health Information Management Association (AHIMA) (2014). HIPAA Privacy and Security Training (Updated). Retrieved on August 2, 2014 from http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_048509.hcsp?dDocName=bok1_048509

American Hospital Association (AHA) (2014). Chartbook – Trends Affecting Hospitals and Health Systems. Retrieved on August 3, 2014 from http://www.aha.org/research/reports/tw/chartbook/ch4.shtml

American Hospital Association (AHA) (2014). Fast Facts on US Hospitals. Retrieved August 3, 2014 from http://www.aha.org/research/rc/stat-studies/fast-facts.shtml

American Hospital Association (AHA) (2014). RAC Auditing Reform is Essential to Fix Urgent, Critical Problems. Retrieved on August 4, 2014 from http://www.aha.org/content/14/issuebrief-rac.pdf

American Medical Association (AMA) (2014, February 12). ICD-10 Cost Estimates Increased for Most Physicians. Retrieved on August 3, 2014 from http://www.ama-assn.org/ama/pub/news/news/2014/2014-02-12-icd10-cost-estimates-increased-for-most-physicians.page

Association of Certified Fraud Examiners (ACFE) (2014). What is Fraud?. Retrieved on August 3, 2014 from http://www.acfe.com/fraud-101.aspx

Association of Certified Fraud Examiners (ACFE) (2012). 2012 Report to Nations. Retrieved on August 3, 2014 from http://www.acfe.com/uploadedFiles/ACFE_Website/Content/rttn/2012-report-to-nations.pdf

Baum, Stephanie (2014, July 23). Children's Hospital CMIO turns entrepreneur to more rapidly detect patient data breaches. Retrieved on August 3, 2014 from http://medcitynews.com/2014/07/childrens-hospital-cmio-turns-entrepreneur-to-prevent-patient-data-breaches/

Beck, Melinda and Wilde Mathews, Anna (2014, August 5). Two Insurers to Pool Medical Records in California. Retrieved on August 5, 2014 from http://online.wsj.com/articles/two-insurers-to-pool-medical-records-in-california-1407211305

Berwick, Donald and Hackbarth, Andrew. Eliminating Waste in US Health Care. doi:10.1001 /jama.2012.362

Brubaker, Harold (2014, July 27). Costs of expanded audits aimed at Medicare fraud hit health-care firms. Retrieved on August 4, 2014 from http://articles.philly.com/2014-07-28/business/52094475_1_medicare-fraud-medicare-spending-medicaid-services

Center for Medicare and Medicaid Services (CMS) (2014). Accountable Care Organizations. Retrieved from http://www.cms.gov/Medicare/Medicare-Fee-for-Service-Payment/ACO/ on August 5, 2014

Center for Medicare and Medicaid Services (CMS) (2014). Breach Notification Rule. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html on August 2, 2014.

Center for Medicare and Medicaid Services (CMS) (2014). Business Associates. Retrieved on August 2, 2014 from http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html

Center for Medicare and Medicaid Services (CMS) (2010, August 31). CMS System Security Plan (SSP) Procedure. Retrieved on August 2, 2014 from http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/SSP_Procedure.pdf

Center for Medicare and Medicaid Services (CMS) (2014, May). Eligible Hospital and Critical Access Hospital Meaningful Use Core Measures. Retrieved on August 3, 2014 from http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/downloads/14_Protect_Electronic_Health_Information.pdf

Center for Medicare and Medicaid Services (CMS) (2014). Health Information Privacy – For Covered Entities and Business Associates. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html on August 2, 2014.

Center for Medicare and Medicaid Services (CMS) (2014). HITECH Act Enforcement Interim Final Rule. Retrieved on August 2, 2014 from http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html

Center for Medicare and Medicaid Services (CMS) (2014). How CMS Enforces the HIPAA Privacy and Security Rules. Retrieved on August 3, 2014 from http://www.hhs.gov/ocr/privacy/hipaa/enforcement/process/howocrenforces.html

Center for Medicare and Medicaid Services (CMS) (2014). Instructions for Submitting Notice of a Breach to the Secretary. Retrieved on August 3, 2014 from http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html

Center for Medicare and Medicaid Services (CMS) (2014). Payment Adjustment for Medicare Subsection (d) Eligible Hospitals. Retrieved on August 3, 2014 from http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/PaymentAdj_HardshipExcepTipsheetforHospitals.pdf

Center for Medicare and Medicaid Services (CMS) (2012, December 18). RAC Program Myths. Retrieved on August 4, 2014 from http://www.cms.gov/Research-Statistics-Data-and-Systems/Monitoring-Programs/Medicare-FFS-Compliance-Programs/Recovery-Audit-Program/Downloads/RAC-Program-Myths-12-18-12.pdf

Center for Medicare and Medicaid Services (CMS) (2014). The Privacy Rule. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/ on August 2, 2014.

Center for Medicare and Medicaid Services (CMS) (2014). The Recovery Audit Program and Medicare. Retrieved on August 4, 2014 from http://www.cms.gov/Research-Statistics-Data-and-Systems/Monitoring-Programs/Medicare-FFS-Compliance-Programs/Recovery-Audit-Program/Downloads/The-Recovery-Audit-Program-and-Medicare-Slides-051313.pdf

Center for Medicare and Medicaid Services (CMS) (2014). The Security Rule. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/ on August 2, 2014.

Center for Medicare and Medicaid Services (CMS) (2014). Transactions & Code Sets Standards. Retrieved on August 2, 2014 from http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/TransactionCodeSetsStands/index.html?redirect=/transactioncodesetsstands/05_codesets.asp

Clark, Cheryl (2012, December 12). Higher Readmission Penalties Linked to Low HCAHPS Scores. Retrieved on August 3, 2014 from http://www.healthleadersmedia.com/page-1/FIN-287372/Higher-Readmission-Penalties-Linked-to-Low-HCAHPS-Scores

Commonwealth of Massachusetts, Division of Banks (2014, June 18). TO THE CHIEF EXECUTIVE OFFICER OF THE FINANCIAL INSTITUTION ADDRESSED. Retrieved on August 2, 2014 from http://www.mass.gov/ocabr/docs/dob/cybersecurityresources.pdf

Crosman, P. (2011, August 1). Chief Risk Officers Rule. *Bank Technology News*, *24*(08), 15. Retrieved from http://go.galegroup.com/ps/i.do?id=GALE%7CA263061422&v=2.1&u=temple_main&it=r&p=ITOF&sw=w&asid=04c65f72dd8dc7b74344dccad399b75c

Daft, Richard (2007). Organization Theory and Design, 9th Edition. Mason, OH: Thomson Higher Education, 2007.

eHealthInitiative (2014, February 26). Integrating Privacy & Security into Organizational Strategy & Culture. Retrieved on August 2, 2014 from http://www.ehidc.org/resource-center/event-summaries/view_document/374-event-summary-integrating-privacy-security-into-organizational-strategy-culture

Federal Financial Institutions Examination Council (FFIEC) (2014). About the FFIEC. Retrieved on August 2, 2014 from http://www.ffiec.gov/about.htm

Federal Financial Institutions Examination Council (FFIEC) (2014). Enforcement Actions and Orders. Retrieved on August 2, 2014 from http://www.ffiec.gov/enforcement.htm

Federal Financial Institutions Examination Council (FFIEC) (2014). Information Security. Retrieved on August 2, 2014 from http://ithandbook.ffiec.gov/it-booklets/management/it-risk-management-process/it-controls-implementation/information-security.aspx

Federal Financial Institutions Examination Council (FFIEC) (2014). IT Booklets. Retrieved on August 2, 2014 from http://ithandbook.ffiec.gov/it-booklets.aspx

Financial Services Information Sharing and Awareness Center (FS-ISAC) (2014). About FS-ISAC. Retrieved on August 2, 2014 from https://www.fsisac.com/about

Financial Services Information Sharing and Awareness Center (FS-ISAC) (2011). Overview of the FS-ISAC. Retrieved on August 2, 2014 from https://www.fsisac.com/~fsisacki/sites/default/files/FS-ISAC_Overview_2011_05_09.pdf

Goldman, T.R. Eliminating Fraud and Abuse. Retrieved on August 3, 2014 from http://www.healthaffairs.org/healthpolicybriefs/brief.php?brief_id=72

HealthIT.gov (2014). Health Information Exchange (HIE). Retrieved on August 4, 2014 from http://www.healthit.gov/HIE

Herman, Bob (2013, February 4). 13 Statistics on Hospital Profit and Revenue in 2011. Retrieved on August 3, 2014 from http://www.beckershospitalreview.com/finance/13-statistics-on-hospital-profit-and-revenue-in-2011.html

(2005), Part Three: The role of the chief risk officer (CRO). J of Healthcare Risk Mgmt, 25: 19–24. doi: 10.1002/jhrm.5600250407

Kissel, Richard (2013, May). Glossary of Key Information Security Terms. http://dx.doi.org/10.6028/NIST.IR.7298r2

Kroll Advisory Solutions (2013). Global Fraud Report Annual Report 2012/13. Retrieved on August 3, 2014 from http://www.kroll.com/library/krl_fraudreport2012-13.pdf

Lassman, David; Hartman, Micah; Washington, Benjamin; et al (2014, May). National Health Spending In 2012: Rate Of Health Spending Growth Remained Low For The Fourth Consecutive Year.
HEALTH AFFAIRS Volume: 33 Issue: 5 Pages: 815-822 Published: MAY 2014

LexisNexis, Inc. (2013). 2013 True Cost of Fraud Study. Retrieved on August 3, 2014 from http://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2013.pdf

Medscape (2014). Protecting Patients' Rights. Retrieved on August 2, 2014 from http://www.medscape.org/sites/advances/patients-rights

New York State Department of Financial Services. Report on Cyber Security in the Banking Sector. Retrieved from http://www.dfs.ny.gov/about/press2014/pr140505_cyber_security.pdf on August 2, 2014.

Otisik, Jon (2011, March 31). To Whom Should the CISO Report? Retrieved on August 5, 2014 from http://www.networkworld.com/article/2228899/cisco-subnet/to-whom-should-the-ciso-report-.html

Payment Card Industry Security Standards Council, LLC (PCI SSC) (2013, November). PCI DSS 3.0. Retrieved on August 2, 2014 from https://www.pcisecuritystandards.org/security_standards/documents.php

Sinno, Michael, Gandhi MD, Snehal, and Gamble, Molly (2011, April 28). 8 Problems Surrounding Meaningful Use. Retrieved on August 3, 2014 from http://www.beckershospitalreview.com/healthcare-information-technology/8-problems-surrounding-meaningful-use.html

Stevens, Lee, and Black, Kate. Patient Matching Findings Released. Retrieved on August 3, 2014 from http://www.healthit.gov/buzz-blog/electronic-health-and-medical-records/patient-matching-findings-released/

United States Department of Commerce (Commerce) (2014). The Financial Services Industry in the United States. Retrieved on August 2, 2014 from http://selectusa.commerce.gov/industry-snapshots/financial-services-industry-united-states

United States Department of Justice (USDOJ) (2014). 978 Health Care Fraud and Abuse Control Program and Guidelines. Retrieved on August 3, 2014 from http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/crm00978.htm#statement

Vincent Oliva, Financial Services Research Leader, Industry,Advisory Services. (2007). Take risk management and compliance to the next level -- as insurers face increasingly onerous regulatory compliance demands, they should make enterprise risk management a high priority and consider appointing chief risk officers. *Insurance & Technology,32*(2), 32. Retrieved from http://search.proquest.com/docview/229288658?accountid=14270

Wex Legal Dictionary (2014). Healthcare Fraud. Retrieved on August 3, 2014 from http://www.law.cornell.edu/wex/healthcare_fraud