Information Risk Management Capability Advancement Model™ (IRMCAM™)

A Clearwater Compliance White Paper

With accompanying...
Clearwater Information Risk Management Capability Advancement Model™ Assessment Tool

Prepared By:
Bob Chaput, MA, CISSP, HCISPP, CRISC, CIPP/US
Mary Chaput, MBA, HCISPP, CIPP/US, CIPM
# Table of Contents

Acknowledgements 3  
Who Will Benefit By Reading this White Paper 3  
Executive Summary 4  
1. Introduction and The Problem We’re All Trying to Solve 6  
- Increasing Risk to Individuals 6  
- Increasing Risk to Organizations 8  
- What’s the Hold Up on Risk Management? 10  
- What Needs to Be Done? 10  
- What is The Specific Problem We Need to Address? 12  
- Why A Maturity Model? 13  
2. Risk Management & Baseball 14  
3. Risk, Risk Management & The Case for Action 15  
4. Clearwater Information Risk Management Capability Advancement Model™ 17  
    - Using the Model 18  
    - Key Risk Management Practice Areas 19  
    - Risk Management Capability Maturity Levels 20  
5. Information Risk Management Capability Maturity Assessment 22  
6. Summary and Next Actions 24  
Contact 27  
About Clearwater Compliance LLC 27  
About the Authors 28  
- Bob Chaput, MA, CISSP, HCISPP, CRISC, CIPP/US 28  
- Mary Chaput, MBA, HCISPP, CIPM, CIPP/US 28  
ENDNOTES 29
Acknowledgements

Clearwater Compliance developed the Information Risk Management Capability Advancement Model™ in collaboration with private and public sector leaders and experts in privacy, security, compliance and information risk management. Clearwater acknowledges the dedication and business risk management expertise of all the organizations and individuals who reviewed our initial drafts and provided the critiques, evaluations, and modifications in order to produce this latest Version 2.1 the Information Risk Management Capability Advancement Model™ white paper. We express our special thanks to our advisory “Kitchen Cabinet” comprising a cross-section of experts representing virtually every sector of the healthcare ecosystem:

1. David Finn | Health IT Officer | Symantec Corporation
2. Adam Greene, JD | Partner | Davis Wright Tremaine LLP
3. Meredith Phillips | Chief Information Privacy & Security Officer | Henry Ford Health System
4. Eric Bergen | Independent Consultant
5. Ian Johansson | Corporate Compliance Officer | Aloha Care Health Plan
6. Sam Homer, Ph.D. | Healthcare Technology Strategist | Health Care Service Corporation
7. Kathy Jobes | Chief Information Privacy & Security Officer | Sentara Healthcare
8. Ed Schreibman | Vice President of Healthcare Compliance | Expert Global Solutions, Inc.
9. Deborah Schlesinger | Director Corporate Risk & Insurance Management | SCAN Health Plan
10. Michelle Caswell, JD | Senior Director – Legal & Compliance | Clearwater Compliance LLC
11. Matt Hanis | Vice President | Lockton
12. Scott Blanchette | Chief Information Officer | Kindred Healthcare
13. Kyle Duke | CIO | TN Division of Health Care Finance & Administration
14. Chris Dansie, Ph.D. | Assistant Professor | University of Utah

Who Will Benefit By Reading this White Paper

The Clearwater Information Risk Management Capability Advancement Model™ enables organizations to evaluate information risk management capabilities consistently, communicate capability levels in meaningful terms, and help make informed decisions about information risk management investments. While this white paper originates from our work in the healthcare sector where much needed improvement in information risk management is underway, the model can be used by virtually any organization in any industry. With the growing need for information risk management to become a board and c-suite agenda item, we include these individuals in our target audience for this white paper:

- Governance leaders (Boards) and C-suite executives who control the allocation of resources and the management of risk in organizations,
- Business Leaders in all operational areas with responsibility for managing organizational resources and operations associated with the best practices of this model, and
- Privacy, security, compliance and information risk management professionals with responsibility for supporting the organization’s information risk management program,
who need to ensure that this information risk management information is communicated in a timely and effective manner to Boards and business leaders and, potentially, with the use of this model.

Executive Summary

While the content of this white paper and the ensuing recommendations are applicable to organizations in all industries, this information risk management white paper is especially important to healthcare organizations and most of their vendors. These organizations that create, receive, maintain or transmit Protected Health Information (PHI) are defined under the Health Insurance Portability and Accountability Act (HIPAA) as Covered Entities (CE) and their Business Associates (BA), and are required by law to protect this information from compromise or potentially suffer considerable consequences.

The risks of a data breach have increased dramatically for all organizations in the healthcare ecosystem. The increase in the adoption of electronic health records (EHR) systems (as a result of government incentives to motivate providers to implement health information technology (HIT) solutions for the purpose of improving health care) has preceded the awareness and understanding of the need, and the methods, for protecting that information. In addition, there is a dimension of increased risk with new modalities of health care services that are creating, receiving, transmitting or storing health information, including Personal Health Records, health kiosks, Personal Digital Assistants (PDAs) and “healthwear” (portable wearable medical technology), not to mention a myriad of new medical devices. The availability of low-cost, high-speed broadband service offered by Google Fiber and other providers may result in additional impermissible access to, and risk for, health information being transmitted. As we evolve to the “Internet of Things”, our approach must be to ensure the “Security of Everything”. Government and private agencies have recently warned of the high level of compromise risk to PHI and the general lack of risk management practiced by organizations to identify and address that risk.

Along with the increasing risk of a data breach is the increasing cost and liability to the organization that suffers such a breach.

Settlements with the Office for Civil Rights (OCR) following a data breach or HIPAA violation have peaked at $4.8 million so far. The Federal Trade Commission (FTC) has imposed 20-year monitoring programs on several healthcare organizations for data breaches on the grounds of “unfair or deceptive
State Attorneys General (SAG) have been given jurisdiction to file civil suits on behalf of their residents over HIPAA privacy and security issues and they are exercising those rights. Lawsuits by affected individuals, and by shareholders of public companies, have also contributed to the high reputational and financial cost of a data breach of healthcare information.

So, given these costly repercussions, why aren’t organizations improving their risk management programs, conducting rigorous risk analyses and making more informed decisions about the appropriate treatment of identified risks to PHI? Unfortunately, risk management programs in the health care industry have historically been focused on clinical risks. There is a general lack of awareness of the level of risk associated with information assets and the potential resulting harm from unauthorized or impermissible use or disclosure. Neither “not knowing” nor “not caring” are acceptable business information risk management strategies.

This white paper and accompanying web-based tools are designed to help organizations have better outcomes in managing information risks. We present important information risk management context and background. We discuss the basic concepts of risk and risk management. We provide a methodology and tools to assist organizations in making more informed risk management decisions and in determining the appropriate level of maturity of their information risk management business process, proportionate to the amount of risk they may face.

The Clearwater Information Risk Management Capability Advancement Model™ (IRMCAM™) and self-assessment capability index are introduced for your immediate adoption in building an efficient and effective information risk management program best suited to meet your organization’s needs. Use of this tool is free during our “invitation-only” BETA trial.
Introduction and The Problem We’re All Trying to Solve

Even though mankind has been managing risk for centuries, few people really understand risk and, therefore, risk management. Over time, numerous international standards organizations have put forth definitions of risk such as:

*The chance of something happening that will have an impact on objectives*\(^6\)

*The effect of uncertainty on objectives*\(^7\)

Organizations, whether for-profit or not-for-profit, set out to plan, operate and deploy business activities and processes to achieve their organizational mission and business objectives. Even the most well planned business activities and well-defined processes carry “risk” to the achievement of these objectives. Historically, risk has been defined in terms of harm, loss or harmful effects. Considering the definitions above, risk may be negative, resulting in loss or harm to the business or its stakeholders or it may be positive because increased benefits or value to an organization can also result from an effect of uncertainty. In this white paper, we concern ourselves with the negative risk associated with loss or harm emanating from the compromise of the confidentiality and/or integrity and/or availability of Protected Health Information (PHI) in any form.

Increasing Risk to Individuals

We can all understand the motivation for illegally obtaining financial information for use in fraudulent purchases or money transfers, but what about health information?

The Federal Trade Commission (FTC) defines medical-identity theft as the fraudulent acquisition of someone’s personal information — name, Social Security number, and health insurance number — for the purpose of illegally obtaining medical services or devices, insurance reimbursements or prescription drugs\(^8\). Cybercriminals looking to capitalize on a bigger payout than that obtained from financial information or identity theft may expedite the targeting of the healthcare industry for access to patients’ PHI. Industry reports reveal medical identity theft has now claimed more than 1.8 million U.S. victims, granting hackers the ability to gain medical services, procure drugs, and defraud private insurers and government benefit programs\(^9\).

“The healthcare industry is not as resilient to cyber intrusions compared to the financial and retail sectors, therefore the possibility of increased cyber intrusions is likely,” according to the Federal Bureau of Investigation in a private notice to healthcare providers, obtained by Reuters.\(^10\)
According to Experian’s 2015 Data Breach Industry Forecast, 42% of the serious data breaches in 2014 were in healthcare and the number is expected to increase in 2015.\footnote{11}

With the expected increase in the Internet of Things\footnote{12} (IoT) from 0.9 billion units in 2009 to 26 billion units in 2020, the number of points of vulnerability for this information to be targeted by hackers is exploding.\footnote{13} And when it comes to the health care, according to Health 2.0, “the increasing ubiquity of health tech interfaces is making these [healthwear] products and services more appealing for long term use for a population where almost 40% is interested in a health tracking device.”\footnote{14} The Experian Data Breach Forecast agrees, concluding, “This expanding number of access points to Protected Health Information (PHI) and other sensitive data via electronic medical records and the growing popularity of wearable technology make the healthcare industry a vulnerable and attractive target for cybercriminals.”\footnote{15}

Incentives for the theft of PHI have typically included selling the information on the black market\footnote{16} for use in defrauding the government, use of the information to gain access to “free” health care for family or friends, and illegal access to narcotics.\footnote{17} More recently, hackers have discovered a new way to capitalize on their efforts by encrypting data in a provider’s environment and holding the password for ransom.\footnote{18} And while details are still sketchy and unverified, delays or refusal to accommodate the request of hackers to pull the release of ‘The Interview,’ (a comedy of an attempt to assassinate Kim Jong Un, the leader of North Korea) have resulted in leaks of information stolen from Sony as proof that the hackers mean business.\footnote{19}

So we know that organizations can suffer financial and reputational harm but what about the victims of medical identity theft? Consider these examples of direct harm or loss to individuals:

- Linda Weaver had two good feet when she opened her mailbox one day. So she was surprised to find a bill for the amputation of her right foot. Weaver, who runs a horse farm in Florida, soon discovered that it wasn’t just a mix-up. Her stolen identity and insurance information had been used to get surgery. She was stuck with the bill—and with a medical record full of incorrect, potentially dangerous information. Even after that, the incorrect records persisted. Two years after her false amputation, Weaver suffered a real heart attack. When she woke up in a hospital room, a nurse asked her what she takes for diabetes—which she doesn’t have.\footnote{20}

- Twelve years ago, when Nikki Burton was 17, she tried to donate blood for the first time. She was denied without explanation. Perplexed, the Portland, Ore. resident called Red Cross headquarters to inquire, only to learn that her Social Security number had been used to receive treatment at a free AIDS clinic in California, rendering her ineligible to donate blood.\footnote{21}

- It all began when Anndorie Sachs (a mother of four who was attending school for a biomedical engineering degree) received a call from the Salt Lake City Division of Child and Family Services (DCFS). It seemed that someone answering Sachs’ name and description had given birth to a premature baby girl, who subsequently tested positive for methamphetamine. The mother had abruptly fled from the hospital leaving the infant and a $10,000 bill behind, and DCFS wanted some answers. Of course, Sachs was not the mother of this child. The baby girl belonged to a woman named Dorothy Bell Moran, who had stolen Sachs’ driver’s license from her car two months before. DCFS, however,
was preparing to submit paperwork to declare Sachs an unfit mother and put her four kids into state custody. Sachs’ 7-year-old daughter was also pulled out of school by DCFS agents and subjected to questioning. Eventually, the issue was cleared up, but Sachs’ problems persisted. Her medical records had been changed to include Moran’s health profile, including her blood type and other information. Sachs can’t even view her own medical records to ensure the information has been changed back — the hospitals involved won’t let her, ironically, because it could compromise the identity thief’s own rights to medical privacy.\(^{22}\)

It is quite possible, even short of medical identity fraud, that information impermissibly disclosed about sexually transmitted disease (STD), abortion, drug or alcohol addiction, mental disorders or conditions or physical defects can create reputational or emotional harm to an individual.

**Increasing Risk to Organizations**

Increasingly, organizations are dealing with new risks to a class of assets that has not traditionally appeared on the financial balance sheet – that is, information assets. It is almost cliché to say it, but without a doubt, these information assets have become the lifeblood of business. There are few, if any, industries in the world unaffected by what has been dubbed “cyber security” risks to these information assets. In the U.S., these risks have become a major concern of financial services, retail, healthcare, utilities and other organizations, in addition to law enforcement agencies and regulators.\(^{21}\) Some recent examples include:

- In October 2013, data from more than 38 million customer accounts was obtained improperly from the software company, Adobe Systems, Inc.\(^{24}\)
- In December 2013, a cyber-attack on Target Corporation resulted in the unauthorized access of payment card data of approximately 40 million Target customers and the personal data of up to 70 million Target customers;\(^{25}\)
- In January 2014, a cyber-attack on Snapchat, a mobile messaging service, exposed a reported 4.6 million user names and phone numbers;\(^{26}\)
- The sustained and repeated cyber-attacks against several large U.S. banks, in which their public websites have been knocked offline for hours at a time;\(^{27}\)
- In March 2014, the U.S. Government Personnel Network\(^ {28}\) was compromised by Chinese hackers targeting the information of tens of thousands of employees who had applied for top-secret security clearances.
- In June 2014, the New York Times reported how cybercriminals are getting better at circumventing firewalls and antivirus programs, and more of them are resorting to ransomware, which encrypts computer data and holds it hostage until a fee is paid;\(^{29}\) and
- In August 2014, Community Health Systems filed an SEC 8-K\(^ {30}\) with the U.S. Securities and Exchange Commission in which it “confirmed that its computer network was the target of an external, criminal cyber-attack that the Company believes occurred in April and June, 2014”. An estimated 4.5 million patients’ personal information was disclosed.

To further educate, and perhaps grab the attention of health care organizations of the need to protect PHI, the Health Information Technology for
Economic and Clinical Health (HITECH) Act has raised the ante significantly as it relates to privacy, security and compliance requirements under the HIPAA Privacy, Security and HITECH Breach Notification regulations. These changes, finalized in a bundle of five regulations known as The Omnibus Final Rule, will likely translate into increased financial, legal, reputational, operational or even clinical risks to any organization with access to PHI. Recent examples of these ramifications can be found on the HHS website under Enforcement Examples and include:

- First copier case: Affinity Health Plan, Inc. agreed to a settlement of $1,215,780 after impermissibly disclosing the PHI of up to 344,579 individuals when it returned multiple photocopiers to a leasing agent without erasing the data contained on the copier hard drives.
- First settlement with a state department: Alaska Department of Health and Social Services agreed to pay $1.7 million after reporting that a USB hard drive possibly containing electronic protected health information (ePHI) was stolen from the vehicle of a DHSS employee.
- First settlement with a county government: Skagit County agreed to a $215,000 monetary settlement following a breach of money receipts when ePHI of seven individuals were accessed by unknown parties after the ePHI had been inadvertently moved to a publicly accessible server maintained by the County.
- Recent settlement with a university: Idaho State University (ISU) has agreed to pay $400,000 to the U.S. Department of Health Human Services (HHS) for violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule. This settlement involves the breach of unsecured ePHI of 17,500 individuals who were patients at an ISU clinic.
- Most recent settlement (December 8, 2014) with a non-profit behavioral health organization: Anchorage Community Mental Health Services (ACMHS), a 5-facility, non-profit organization providing behavioral health care services to children, adults and families in Anchorage, has agreed to pay $150,000 to HHS and adopt a corrective action plan for the malware breach of unsecured ePHI affecting 2,743 individuals. The investigation determined that ACMHS had failed to identify and address basic risks in outdated and unsupported software and had not implemented purchased policies and procedures.
- Largest HIPAA settlement to date: New York and Presbyterian Hospital (NYP) and Columbia University (CU) agreed to pay $4,800,000 after reporting the disclosure of the ePHI of 6,800 individuals, including patient status, vital signs, medications, and laboratory results when a physician employed by CU who developed applications for both NYP and CU attempted to deactivate a personally-owned computer server on the network containing NYP patient ePHI.

In none of the cases above, and as of this writing, has the increased penalty amounts under the Civil Monetary Penalty System resulting from the HITECH Act been used except in one case. The dollar amounts above represent negotiated settlements rather than the application of the new, significantly more expensive CMPS. To date, only Cignet Health of Prince George’s County, MD has had a CMP of $4.3 million imposed for not responding to individual requests for access to their health records nor to “OCR’s written notification of the investigations, numerous follow-up attempts to contact Cignet by telephone, or to two subsequent letters ... informing
Cignet of its obligation at 45 C.F.R. § 164.524 to provide the individuals access to obtain a copy of the protected health information ...”.

While cyber security threats from external adversarial sources are increasing, they are not the only concerns to be addressed by a CE or BA. Healthcare breach data from the Department of Health and Human Services (DHHS) “wall of shame” website supports the fact that an organization’s own employees are historically more often the root cause of privacy, security or compliance violations than external, and adversarial threat sources. As of December 5, 2014, of the 1,170 breaches affecting 41.5 million individuals, only 7% of the number of breaches, and 7% of the number of individuals affected, were due to “Hacking/IT Incidents”; while 93% of the breaches and 93% of the number of individuals affected were due to other causes, such as unintentional or intentional activities of the workforce including:

- Theft/Loss (64% of the # of breaches; 72% of the # of individuals)
- Unauthorized Access and Disclosures (16% of the # of breaches; 12% of the # of individuals)
- Improper Disposal of PHI (4% of the # of breaches; 2% of the # of individuals) and
- All Other/Unknown (9% of the # of breaches; 7% of individuals)

While cyber security threats from external adversarial sources are increasing, they are not the only concerns to be addressed by a CE or BA.

What’s the Hold Up on Risk Management?

To reduce the likelihood and impact of the compromise of any sensitive information, organizations must implement a balanced information risk management program that invests in and implements reasonable and appropriate policies, procedures, people programs (such as background checks, training and disciplinary actions for non-compliance) and safeguards or controls.

Yet, organizations struggle to implement such programs and address these new information risks for a variety of reasons, among them:

1) Frequently there is not strong alignment between the business strategy and the organization’s information risk management strategy. In May 2014, Rand Health prepared a research report for the Office of the National Coordinator for Health Information Technology entitled “Promoting Patient Safety Through Effective Health Information Technology (HIT) Risk Management”. Among other findings about lackluster risk
management surrounding HIT, the research report asserts:

“With few exceptions, awareness of the safety risks introduced by health IT is limited. The traditional departmental ‘silos’ between risk management, IT, and quality and safety management may impede the ability of organizations to recognize and respond to health IT safety risks.”

2) Risk management is not a well-understood or appreciated business process, and, therefore is generally practiced in a very ad hoc and inconsistent manner. As noted by the Committee of Sponsoring Organizations of the Treadway Commission (COSO):

“In the aftermath of the financial crisis, executives and their boards realize that ad hoc risk management is no longer tolerable and that current processes may be inadequate in today’s rapidly evolving business world.” However, especially for nonfinancial companies that may be relatively new to these topics, enhancing risk management can be a somewhat daunting task.

3) Health care organizations have not been as focused on the risk to health care data since, before the move to electronic data, the primary security measures were locked doors, file cabinets and desk drawers. In April 2014, the FBI released an alert warning to healthcare providers of a high level of risk for data security as adoption of electronic health records accelerates in a Private Industry Notification (PIN) entitled “Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain”. The PIN warns:

“Because the healthcare industry is not as ‘resilient to cyber intrusions [as] the financial and retail sectors, therefore the possibility of increased cyber intrusions is likely”

4) Boards, governance bodies and executives are not as engaged, supportive and, ultimately, as responsible as they should be. In a June 2014 speech, SEC Commissioner Luis A. Aguilar spoke on “Cyber Risks and the Boardroom” at a New York Stock Exchange Conference in New York. He observed:

Clearly, boards must take seriously their responsibility to ensure that management has implemented effective risk management protocols. Boards of directors are already responsible for overseeing the management of all types of risk, including credit risk, liquidity risk, and operational risk – and there can be little doubt that cyber-risk also must be considered as part of board’s overall risk oversight. The recent announcement that a prominent proxy advisory firm is urging the ouster of most of the Target Corporation directors because of the perceived “failure…to ensure appropriate management of [the] risks” as to Target’s December 2013 cyber-attack is another driver that should put directors on notice to proactively address the risks associated with cyber-attacks.

What Needs to Be Done?

Our privacy, security and compliance focus is on safeguarding “information assets”. Because we live with a dynamic, constantly changing “threat landscape”, protecting all sensitive information assets (e.g., Protected Health Information (PHI), Personally Identifiable Information (PII), credit card data, trade secrets and other company proprietary data) requires a well-honed risk management process. The risk management process requires identifying all these assets and
all the possible exposures. Identifying all these exposures means we must understand all the possible threats to our information assets, the weaknesses we may have in protecting them, and the controls that we have (or have not) put in place to help mitigate the exploitation of these weaknesses. The risk management process requires an organization to continuously assess the risk environment, prioritize and address new or changing identified risks, and monitor or strengthen controls that have been implemented to mitigate the possibility of loss of, or harm to, these information assets.

In its document “Guidance on Risk Analysis Requirements under the HIPAA Security Rule”\(^42\), HHS / OCR have guided healthcare organizations to follow the risk management approach outlined in the NIST Security Framework and specifically found in key Special Publications (SP) such as the following:

- NIST SP800-30 Revision 1 Guide for Conducting Risk Assessments\(^43\)
- NIST SP800-39-Managing Information Security Risk\(^45\)

**What Is The Specific Problem We Need to Address?**

Loss or harm to information assets occurs when there is a compromise of the confidentiality of information (e.g., impermissible use or disclosure), integrity of information (e.g., unauthorized change or destruction) or availability of information (e.g., inaccessible or unavailable). Sometimes referred to as the Confidentiality - Integrity - Availability (C-I-A) triad, these three attributes represent the foundational requirements of any information protection program, and the basis of the information risk management process in every industry.

A compromise may result in significant loss or harm to your organization and/or to any of your stakeholders – patients, members, residents, customers, suppliers, employees, and/or investors. In healthcare, such compromises could become a matter of life or death for the patient, health plan member or facility resident. For the organization, the harm can include financial penalties and fines, reputational damage, lawsuits or other enforcement actions such as corrective action plans, government monitoring and/or state bans.

So in summary, the problem we’re all trying to solve is the prevention of compromise of the confidentiality and/or integrity and/or availability of any sensitive information with which we have been entrusted. In order to prevent such compromises, we need to first identify all the risks to the information and then assess the relative likelihood and impact of each such risk. Once we identify, risk-rate and prioritize each risk, we can then make informed decisions about how to address those risks – do we accept

A balanced and appropriately mature information risk management program is the solution to this critical exercise and can even result in a competitive advantage for the organization.
the risk, avoid the risk, mitigate the risk or transfer the risk.

A balanced and appropriately mature information risk management program is the solution to this critical exercise and can even result in a competitive advantage for the organization. In this white paper and accompanying web resources, we set out to help organizations make the most informed decisions on how mature their information risk management programs should be. We explain the concepts of risk, risk management and the case for action. We introduce the idea of an information risk management Capability Advancement Model and how it can be used as an assessment, decision making and action-planning tool. We cover what constitute the most key risk management practices and using these, describe various risk management Capability Advancement Model levels. And, we provide a self-assessment tool that may be used to start the process of implementing the balanced information risk management program for one's organization.

Why a maturity model?

The use of a maturity model allows an organization to have its methods and processes assessed according to management best practices, against a clear set of external benchmarks. Maturity is measured by the designation of a particular “Maturity Level”. A maturity level assessment of an organization’s risk management program will provide the following benefits:

- Establish a current Maturity Level, with precise recommendations on how to improve
- Provide the ability for organizations to compare their Maturity Level with other organizations, or other parts of their own organization
- Trend improvements on process maturity self-assessments through
  - A consistent set of questionnaires and scoring
  - Independently verified and certified scoring
- Allow measurement against an independently held set of “benchmarks”.

46
Think about the types of baseball teams you may have encountered over the course of time. Tee-ball teams typically organized for children aged 4 to 8, Little League teams that may include children up to age 16, American Legion teams, Babe Ruth teams, high school teams, college teams, amateur teams, semi-pro teams, minor league teams and ultimately professional Major League teams.

We use this analogy because it is apparent that there are different levels of maturity between these various teams. Compare a Little League team to a Major League Baseball team:

<table>
<thead>
<tr>
<th></th>
<th>LITTLE LEAGUE TEAM</th>
<th>MAJOR LEAGUE BASEBALL TEAM</th>
</tr>
</thead>
</table>
| What happens when a ball is hit to a Little League team? | • Everyone runs around at random  
• They might do the right thing, or they might not  
• The next time the ball is hit in the same place, they may do something different | • Everyone moves in a coordinated fashion, based on practicing that play many times  
• Sometimes they fail to make the right play, but they almost always try to do the right thing |
| What happens when the team loses a star player? | • Little League team gets much worse | • Professional team usually has someone waiting to fill in |
| What happens when there’s a bad play? | • Little League players don’t know what went wrong, or they blame each other | • Professional teams discuss their play and look for ways to improve. “The next time there is an infield hit with 2 outs, let’s do this instead.” |

A Major League Baseball team is more “mature” than a Little League team. A Major League Baseball team has self-perpetuating quality. They make good plays, develop new players like themselves, use the latest ‘technology’, hone ‘processes’ and find ways to improve and make better plays.

When it comes to information risk management in your organization, it is not automatically the case that you need to play “Major League Baseball” – possibly, but not automatically! What is important is that a conscious, informed decision is made about the level of maturity at which your organization needs to “play” information risk management:

- Is Little League good enough?
- Given the sensitive information you handle, is semi-pro maturity more appropriate?
- How good does your team have to play?
- How mature does your risk management process need to be?

This white paper and accompanying web solutions are designed to help you. We present and suggest you embrace the Clearwater Information Risk Management Capability Advancement Model™ (IRMCAM™). We encourage you to complete a self-assessment or independent assessment, and purposely decide what level of risk management maturity is best for your organization. We also ask you to consider how mature your competition is when it comes to information risk management.
Historically, risk has been regarded solely as a negative concept (i.e., something bad may happen) that organizations typically tried to ignore, avoid or transfer to others. Increasingly, information risk is recognized as a fact of life that must be “owned” and be dealt with based on informed decision-making. If we understand this risk and how it is caused and influenced, we can change its composition so that we are more likely to achieve our organization’s objectives - maybe even faster, better, cheaper and with better outcomes. Understanding risk and taking action to change its composition is called “risk response.” Good risk response and overall risk management can occur only when organizations recognize that risk management is an important business process and that, like baseball, it can be addressed with different levels of maturity.

Risk is implicit in all decisions we make: how we make those decisions will affect how successful we are in achieving our objectives. Good decision making is, in turn, an integral part of day to day operations and nowhere is it more prominent and critical in an organization than at times of change and when responding to external developments. The changes that the healthcare industry is undergoing now are unprecedented. New methods of delivery and patient communication, reimbursement for improved quality and patient safety, enrollment through public and private exchanges (just to name a few), have all resulted in increasing requirements, expanding service providers and proliferating amounts of electronic health data. The magnitude and nature of these changes are why information risk management is so important to organizations today.

Often captured under the sexier “cyber security” banner, although more numerous and dangerous than ever, these information risks are not new. We have long been concerned with the confidentiality, integrity and availability of information. What’s new is that cyber security is becoming an even more important concern in both the private and public sectors, and for good reason. Law enforcement and financial regulators have stated publicly that cyber-attacks are becoming both more frequent and more sophisticated. The issues are not restricted to financial services, retail or other industries.

Of course, information risk management is not simply about cyber-attacks. Information risk management requires
order, process and discipline. We base our approach on the NIST Security Framework and have developed the Clearwater Information Risk Management Life Cycle based on NIST Special Publication 800-39 Managing Information Security Risk.

The information risk management life cycle includes, but is not limited to framing or characterizing risks, standing up a process for risk management, establishing the organization’s risk appetite (willingness to pursue risk to achieve objectives) and risk tolerance (willingness to endure risk to achieve objectives) and putting it all into practice.

For many, if not most organizations, information risk management is little more than ‘arts and crafts’ executed at the Little League or even Tee-ball league level. For too few others, information risk management has become ‘science and engineering-based’, executed at the professional Major League Baseball level.

We do not advocate that every organization’s risk management program needs to be as mature as a Major League Baseball team. We advocate that organizations assess at what maturity level their programs are operating today and then make a conscious, informed decision about whether that is good enough. And, if not good enough, to decide at what level of maturity they need to operate and then set forth a plan to get there.
The Clearwater Information Risk Management Capability Advancement Model™ (IRMCAM) is designed to create a framework against which an organization can shape its information risk management program.

The accompanying web solutions, including the Clearwater Information Risk Management Capability Advancement Model Index™ (IRMCAMI™) described below will help organizations determine their current level of information risk management maturity and then set an appropriate course of action for improvement, if appropriate.

Just like baseball teams, mature risk-aware organizations are different from immature risk-aware organizations. IRMCAM strives to capture and describe these differences. IRMCAM strives to create organizations that are “mature”, or more mature than before applying IRMCAM. The model describes six levels of risk management process maturity based on best practices in five key areas. In other words, consistent with capability levels and practice attributes defined in ISO/IEC 15504 Process Assessment Standard that applies to software life cycle processes, we have created a model that allows an organization to determine its current achieved information risk management process capability level using five key practice attributes.

Summarized here and described further below, the Key Risk Management Practice Areas are:

- Risk Management Governance, Awareness of Benefits and Value
- Risk Management People, Skills, Knowledge & Culture
- Risk Management Process, Discipline, & Repeatability
- Risk Management Use of Standards, Technology Tools / Scalability
- Risk Management Engagement, Delivery & Operations

<table>
<thead>
<tr>
<th>RISK MANAGEMENT IMPLEMENTATION MATURITY</th>
<th>Incomplete-0</th>
<th>Performed-1</th>
<th>Managed-2</th>
<th>Established-3</th>
<th>Predictable-4</th>
<th>Mature-5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Engagement, Delivery &amp; Operations</td>
<td>None</td>
<td>Some</td>
<td>Have</td>
<td>Formal</td>
<td>Formal</td>
<td>Embedded</td>
</tr>
<tr>
<td></td>
<td></td>
<td>insufficient resources</td>
<td>framework &amp; active when time permits</td>
<td>program</td>
<td>in decision making, CPI</td>
<td></td>
</tr>
<tr>
<td>Use of Standards, Technology Tools/Scalability</td>
<td>Not Using</td>
<td>Aware but not Formalized use</td>
<td>Using selectively</td>
<td>Using, repeatable results</td>
<td>Regular use, outcomes consistent</td>
<td>Sound understanding, good use of tools</td>
</tr>
<tr>
<td>Process, Discipline, &amp; Repeatability</td>
<td>No PnPs, formal practices</td>
<td>Some execution, no records or docs</td>
<td>Some PnPs, docs; not consistently followed</td>
<td>Formal PnPs and docs, widely followed</td>
<td>Robust, widely adopted PnPs</td>
<td>Formal, continuous process improvement</td>
</tr>
<tr>
<td>People, Skills, Knowledge &amp; Culture</td>
<td>Little knowledge</td>
<td>Some risk skills training as parts of organization</td>
<td>Good understanding across parts of organization</td>
<td>Knowledge across most of organization</td>
<td>Sound knowledge of discipline and value</td>
<td>High degree of knowledge, refinement</td>
</tr>
<tr>
<td>Governance, Awareness of Benefits &amp; Value</td>
<td>Unsure of benefits; no executive focus</td>
<td>Aware but not clear on benefits</td>
<td>Aware of some benefits</td>
<td>Aware of most benefits; value realized</td>
<td>Aware of benefits and deployed across the organization</td>
<td>Incorporated into business planning and strategic thinking</td>
</tr>
</tbody>
</table>
Information risk management process capability levels are defined in more detail below as well, and are listed here:

- Level 0 - Incomplete
- Level 1 - Performed
- Level 2 - Managed
- Level 3 - Established
- Level 4 - Predictable
- Level 5 - Mature

The purpose of the Clearwater IRMCAM™, as with all Capability Advancement Models in general, is to assist an organization in rating itself on a scale from the least mature level to the most mature level. These levels within the Capability Advancement Model are designed to allow an organization to identify descriptions of its current and possible future states. Capability maturity is not a competition with other organizations. The model and accompanying web solutions identify where an organization’s risk management program stands in relation to certain activities or practices and suggests how to set priorities for improvements.

In assessing capability maturity, these following attributes are often considered. Is the process...

- Proactive?
- Adaptable?
- Consistent?
- Predictable?
- Measurable?
- Governed?
- Controlled?
- Automated?
- Continuous Process Improvement (CPI)-based?
- Standards-based?

**Using the Model**

Organizations may use the model to complete a self-assessment or engage a third party to assist them with the assessments. In the former case, you would train your own team in IRMCAM, then conduct internal assessments. For a large organization with many exposures, this former approach could have a big payoff. In the latter case, an organization might hire a 3rd party IRMCAM assessor to conduct a formal evaluation. Using a 3rd party may help win management attention, ensure an independent, objective evaluation and demonstrate good faith intent to customers and regulators.

Overall, an organization would use the model to:

- Determine where its information risk management program currently stands;
- Decide where it needs to be; and,
- Set a plan of action to get there!
Key Risk Management Practice Areas
In this section, we briefly define the most key information risk management practices that characterize process maturity and, ultimately, the most effective and efficient risk management outcomes.

Risk Management Governance, Awareness of Benefits and Value
Governance is usually defined as a system of processes and controls that ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-upon enterprise objectives to be achieved; setting direction through prioritization and decision making; and, monitoring performance and compliance against agreed-upon direction and objectives.

Risk Management Governance is a strategic business practice area that is part of overall governance and ensures that:

- Risk management activities align with the enterprise’s opportunity and loss capacity and leadership’s subjective tolerance of it; and,
- The risk management strategy is aligned with the overall business strategy

When fully matured, enterprise decisions consider the full range of (risk) opportunities and consequences.

Risk Management People, Skills, Knowledge & Culture
The success of any business strategy, process, program or initiative ultimately rests with individuals with the right skills, knowledge, experience and passion about the subject matter. The Risk Management People, Skills, Knowledge & Culture practice area is one of the most key areas. If Risk Management Governance is about board and senior executive engagement, leadership and support, Risk Management People, Skills, Knowledge & Culture is about skilled information staff and the creation of a risk-aware culture.

Organizations with matured Risk Management People, Skills, Knowledge & Culture have a high degree of knowledge of the risk management discipline across the organization and make informed risk-aware decisions.

Risk Management Process, Discipline & Repeatability
Generically, a process is defined as a set of interrelated or interacting activities, which transforms inputs into outputs. Each process has customers and other interested parties (who may be either internal or external to the organization), with needs and expectations about the process, who define the required outputs of the process.

Like any other process, an organization’s Risk Management Process should be aligned with the objectives, scope and complexity of the organization, and should be designed to add value to the organization.

Organizations with an overall mature Risk Management Process have formal, well-documented and consistently followed policies and procedures around risk
management. These policies and procedures help ensure a risk management process that is predictable, measurable, controlled, CPI-based, and standards-based.

**Risk Management Use of Standards, Technology Tools and Scalability**

Risk Management Use of Standards, Technology Tools and Scalability enable enterprise risk portfolio management, automation of risk management workflows such as the critical risk analysis workflow, and key activities and controls monitoring. More importantly, tools and technology are essential for scalability. Any set of information assets that is not trivial will possess a large threat surface and a multiplicity of vulnerabilities.

Technology becomes critical when one considers the number of combinations and permutations of asset-threat-vulnerability ‘triples’ that need to be examined in a thorough risk analysis. Without automation and technology, it is simply not possible to complete a comprehensive, rigorous risk analysis and keep it up to date.

Many organizations attempt to build their own surveys and spreadsheets to complete risk analyses. These home-grown solutions rarely scale, are not updated with ever-changing threats and vulnerabilities and provide no way in which to stand up and sustain an ongoing risk management program.

Using standards-based (e.g., NIST-based) automation means adopting tools that have been used more broadly by multiple organizations and have received scrutiny from enforcement agencies. The advantage of using standards-based technology, especially when guided by regulation to do so, is recognition and evaluation by a larger community.

Organizations mature in their use of Risk Management Use of Standards, Technology Tools and Scalability by using standards-based tools consistently across the organization and are realizing predictable, repeatable results.

**Risk Management Engagement, Delivery & Operations**

Risk Management Engagement, Delivery & Operations is about the extent to which the organization is actively engaged in and has deployed risk management practices. Organizations that are most mature have formally adopted risk management such that it is a formal program and risk issues are embedded in all decision making. There is one, consistently used framework and the organization works to continuously improve its risk management program and processes.

Large or complex organizations may require a hierarchy of information risk management plans. It is essential to have a risk management plan for the whole organization that describes the broad strategies to be pursued. However, requiring departments to develop their own plans can enforce accountability for risk management within an organization or divisions to develop their own risk management plans, showing how they will integrate and embed risk management processes into their own processes and practices. The most mature organizations understand the need for
hierarchy and delegation of responsibility.

**Risk Management Capability Maturity Levels**

We have created a model and assessment solutions that allow an organization to determine its current achieved information risk management process capability level using the five key best practice attributes previously discussed. Process capability maturity levels are described briefly in this section.

**Level 0 - Incomplete**
Anything goes. No awareness or recognition of value of risk management exists. No governance exists. Practices are ad-hoc and chaotic. Risk decisions lack credible information.

**Level 1 - Performed**
Any risk practice that may exists, varies. No risk appetite or tolerance has been stated. The organization has some successes, but will also have failures and badly missed risks.

**Level 2 - Managed**
Some risk management processes are defined, documented & practiced. Some people are trained in them. Groups across an organization may use different processes.

**Level 3 - Established**
There is some awareness to manage risk. Board-issued guidance exists to some extent. Risk management processes are consistent and known across the whole organization. There are emerging champions and leaders.

**Level 4 - Predictable**
Risk management is viewed as business enabler. Board sets risk appetite and risk tolerance. Predictive risk scenarios are used.

**Level 5 - Mature**
Risk is considered in all decisions. Continuous process improvement is present. Experimenting with new methods and technologies is commonplace. Real-time continuous monitoring of risk events is standard. Processes and tools are changed when something works better.
To assist organizations in determining their current level of maturity within the Clearwater IRMCAM™, Clearwater Compliance has developed a web-based assessment tool. We examine each of the five Key Risk Management Practice Areas:

- Risk Management Governance, Awareness of Benefits and Value
- Risk Management People, Skills, Knowledge & Culture
- Risk Management Process, Discipline, & Repeatability
- Risk Management Use of Standards, Technology Tools / Scalability
- Risk Management Engagement, Delivery & Operations

In each practice area, we pose a series of questions relevant to that key risk management practice and rate on a six-point rating scale:

- Not adopted or implemented or achieved (0% or maturity 0)
- Minimally adopted or implemented or achieved (20% or maturity 1)
- Partially adopted or implemented or achieved (40% or maturity 2)
- Largely adopted or implemented or achieved (60% or maturity 3)
- Almost adopted or implemented or achieved (80% or maturity 4)
- Fully adopted or implemented or achieved (100% or maturity 5)

The questions are designed to suggest specific areas of improvement for organizations developing action plans to improve their maturity level.

The Clearwater Information Risk Management Capability Advancement Model Index™ (IRMCAMi) is a web-based survey tool that enables an organization to assess the current level of information risk management maturity.

Using the results from the web-based survey tool, we determine a Risk Management Capability Advancement Model Index™ or score.

The assessment tool is currently a free web-based survey instrument. Through the questions in each of the five Key Risk Management Practice Areas, organizations will better understand risk management best practices. The questions will serve to suggest specific,
tangible actions that organizations may wish to undertake to improve their risk management processes.

The scores for an organization are presented for each of the five Key Risk Management Practice Areas and overall. As we’ve indicated throughout this white paper, Risk Management Capability Maturity is not a one-size-fits-all. The baseball analogy is useful in helping to think about maturity required in your organization vis-à-vis the business risks you may face in handling any sensitive information including PHI, PII, trade secrets, etc.

As an example, an organization’s score may be represented as shown below:

![Score Table]

Please contact us if you are interested in participating in the Beta Test for the Clearwater Information Risk Management Capability Advancement Model Index™ (IRMCAM™).

Please add communications@clearwatercompliance.com to your address book to ensure your invitation reaches your inbox.

Use of this tool is free during our invitation-only BETA trial.
Summary
The guidance provided in this white paper is intended to assist organizations in establishing, operationalizing and maturing their information risk management programs. All of the information risk management maturity principles presented here are applicable to the protection of any sensitive information whether it is personally identifiable information (PII), PHI, or company trade secrets.

In all cases, every organization must aim to ensure the confidentiality, integrity and availability of that information if not to their own benefit, then most certainly to that of their customers and/or patients.

This guidance is not intended to replace information risk-related activities, programs, or processes undertaken by an organization but rather help ensure that an appropriately rigorous and sustainable program is established in an informed manner. Because the very composition of risk (i.e., assets, threats, vulnerabilities, controls) is dynamic, the program to respond to risks must be dynamic as well. If our objective is to prevent or mitigate the compromise of the confidentiality, integrity and availability of our sensitive information, we must be able to change the composition of these risks in some manner to reduce loss or harm. Such an objective needs to be approached systematically and programmatically.

The Clearwater Information Risk Management Capability Advancement Model™ (IRMCAM) presented should assist organizations by providing benchmark levels of maturity against which an organization can evaluate their current level of capability of its practices, processes, and methods and set goals and priorities for improvement. For organizations that have worried about their staff’s lack of expertise to conduct other frameworks, this model provides a pathway to information for both the least and the most experienced staff member.

Over time, with greater adoption of this model in the healthcare and other industries, we intend to build benchmark data so that organizations can assess their performance against other organizations using this tool.
Next Actions
Each organization will choose its own approach to the use an adoption of the Clearwater Information Risk Management Capability Advancement Model™ presented in this paper. As a starter set of specific, tangible next actions, we encourage consideration of the following iterative process:

1. **Prepare to use the Clearwater Information Risk Management Capability Advancement Model™ (IRMCAM™).** Engage an outside facilitator or prepare to complete a self-assessment. Socialize this white paper among peers and “intended audiences” presented in an earlier segment. Complete an initial Clearwater Strategic “Business and Information Privacy, Security and Compliance Program” AlignmentCheck™ to begin to raise conscientiousness to the matter of information risk management.

2. **Set the desired information risk management maturity level for the organization.** Identify a cross-section of Board, executives, management, staff and key stakeholders to form an Assessment Team. Use the Clearwater IRMCAM™ to determine the level at which the organization must operate (e.g., Level 0 - Incomplete, Level 1 - Performed, Level 2 - Managed, Level 3 - Established, Level 4 - Predictable, Level 5 – Mature). Among other factors, consideration must be given to the overall business mission and strategy, nature and amount of sensitive information, the current inherent information risks of the organization and the resources of the organization.

3. **Complete the Clearwater IRMCAM™ tool.** Have each member of the assessment team complete the assessment survey tool. Upon completion of the assessment, a report is generated that shows maturity indicator level results for each best practice area on a scale of zero (0) to five (5). This assessment report provides a picture of the current state of best practices relative to the model. The individual best practice area scores and overall score should be discussed the assessment team. Confirm and agree upon the current maturity level of the organization.

4. **Identify any gaps that may exist between the desired state of maturity and the current state.** Each of the five best practices areas - e.g., i) Governance, Awareness of Benefits and Value; ii) People, Skills, Knowledge & Culture; iii) Process, Discipline, & Repeatability; iv) Use of Standards, Technology Tools / Scalability; and, v) Engagement, Delivery & Operations - will be scored as well as the overall current state of maturity. Use the individual best practices areas and the overall score to identify gaps in practices.

5. **Assess all identified gaps that may exist between the desired and the current state.** Assess whether these gaps represent meaningful and important changes for the organization. Evaluate whether addressing these gaps will result in better overall risk management outcomes. As stated many times, the Clearwater IRMCAM™ is not intended to suggest that risk management capability and maturity is a “one size fits all”. Typically,
it is not optimal for an organization to strive to achieve the highest level of maturity in all best practices areas. An organization should focus on those gaps that will enable it to best meet its business objectives and information risk management strategy.

6. **Rank order identified gaps and remediate the highest priority gaps.**
   After all gaps are identified and analyzed, the organization should prioritize the actions needed to fully implement those practices that enable achievement of the desired capability in specific best practices areas. The prioritization should be done considering the criteria provided above, such as the overall business mission and strategy, the nature and amount of sensitive information, the current inherent information risks of the organization and the resources of the organization. A simple “payoff matrix” (effort vs. payoff) or a more formal cost-benefit analysis may be used to help prioritize most important next actions. Once priorities are established, prepare and execute on a plan to remediate the identified gaps.

7. **Document results and repeat the assessment periodically.**
   With the ongoing changes to the composite elements of risk to an organizations’ information assets, threats, vulnerabilities and controls, it is critical to continue to re-evaluate an appropriate level of information risk maturity and to re-assess the organization’s current state of maturity against that level. These re-evaluations and re-assessments should also be driven by any significant organizational, operational and technological changes in an organization.
Contact

Clearwater Compliance LLC
Phone: 800-704-3394
Web: http://www.clearwatercompliance.com
Email: info@clearwatercompliance.com
Twitter: @ClearwaterHIPAA

About Clearwater Compliance LLC
Clearwater Compliance creates value by assisting healthcare organizations establish, operationalize and mature their information privacy, security, compliance and information risk management programs. Led by veteran, C-suite healthcare executives, Clearwater provides a comprehensive set of capabilities, including by-the-regs HIPAA-HITECH compliance software and tools, risk analysis and management software, professional services, and a variety of educational events and resources.

Clearwater works with healthcare organizations and business associates that are serious about safeguarding the privacy and security of Protected Health Information (PHI) and that are committed to a continuous process improvement approach to managing information risk. Among its varied and loyal customer base, Clearwater serves covered entities ranging in size from major integrated healthcare systems and health plans to large hybrid entity retailers to specialty clinics and small medical practices. Business associate customers include law firms, consulting companies, third party administrators, medical billing companies, software hosting organizations, wellness and data analytic companies and many more, from Fortune 100 companies to healthcare startups. Find out more about our HIPAA compliance and information risk management software, solutions, education events and professional services at clearwatercompliance.com or connect with us via Twitter: @ClearwaterHIPAA
About the Authors

**Bob Chaput, MA, CISSP, HCISPP, CRISC, CIPP/US**

Over the past 35 years, Mr. Chaput has worked as an educator, an executive and an entrepreneur. He has assisted businesses and individuals in developing highly secure information technology (IT) strategies that are tightly linked with their business strategies and goals. Given world events, increasingly more stringent security, privacy and compliance regulations around safeguarding personal and healthcare information (PII and PHI) along with increased business dependency on technology, his passion and focus is in helping organizations establish, operationalize and mature their information risk management programs.

Bob is no stranger to managing and protecting large amounts of data – his experience includes managing some of the world’s largest HR, benefits and healthcare databases, requiring the highest levels of security and privacy. His business career spans many years of increasingly greater responsibility for all aspects of regulatory compliance and information security, with 25+ of those years covering the highly data-regulated healthcare industry. As an educator, he has continued to expand and update his knowledge base through postgraduate study, earning professional certifications and participating in professional healthcare and other organizations.

**Mary Chaput, MBA, HCISPP, CIPM, CIPP/US**

Mary Chaput, MBA, HCISPP, CIPM, CIPP-US, serves as Chief Financial and Compliance Officer for Clearwater Compliance, LLC. Mary’s career includes serving 10 years as Executive Vice President and Chief Financial Officer for Healthways, Inc. (NASDQ: HWAY). Mary was responsible for enterprise risk management, including finance, legal, investor relations and regulatory compliance. As Compliance Officer, Mary oversaw the protection of 1.5 petabytes of health data belonging to 45 million Americans.

Before joining Healthways, Mary held the position of Vice President and Chief Financial Officer for ClinTrials Research, a public contract research organization conducting clinical trials for pharmaceutical and biotech companies. Her 35 years of international and domestic business experience spans the healthcare, information services, manufacturing and venture capital consulting industries. A graduate of the General Electric Financial Management Program, Mary earned her MA in Mathematics from Russell Sage College and MBA from State University of New York, Albany.
Endnotes

1 See 45 CFR 860.103 Definitions - http://www.ecfr.gov/cgi-bin/text-idx?SID=3ea90d87e6a4d7c8d48b52696da93&node=45:1.0.1.3.75.1.27.3&rgn=div8

2 See Department of Health and Human Services web site - http://www.hhs.gov/ocr/privacy/

3 ibid

4 ibid

5 “The Impact of the Internet of Things on Data Centers”: https://www.gartner.com/doc/2627920

6 http://www.standards.co.nz/news/standards-information-risk-management/ - AS/NZS 4360 Risk management, was first published in 1995. After AS/NZS 4360 was last revised in 2004, the joint Australia/New Zealand committee DB-007 decided that rather than undertake a similar revision in 2009, it would promote the development of an international standard on risk management, which could then be adopted locally.


12 The Internet of Things (IoT) is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment. http://www.gartner.com/it-glossary/internet-of-things/

13 “Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020” - http://www.gartner.com/newsroom/id/2636073


19 Hackers have allegedly ordered Sony to can “The Interview” - http://www.itpro.co.uk/security/23593/sony-pictures-hack-studio-exec-ordered-to-cancel-ant-north-korea-film


23 For example, the Director of the Federal Bureau of Investigation (FBI), James Comey, said last November that “resources devoted to cyber-based threats will equal or even eclipse the resources devoted to non-cyber based terrorist threats.” See, Testimony of James B. Comey, Jr., Director, FBI, U.S. Department of Justice, before the Senate Committee on Homeland Security and Governmental Affairs (Nov. 14, 2013), available at http://www.house.senate.gov/hearings/threats-to-the-homeland. See also, Testimony of Jeh C. Johnson, Secretary, U.S. Department of Homeland Security, before the House Committee on Homeland Security (Feb. 26, 2014) (“This must continue efforts to address the growing cyber threat to the private sector and the ‘gov’ networks, illustrated by the real, pervasive, and ongoing series of attacks on public and private infrastructure.”), available at http://docs.house.gov/meetings/HH/HH00/20140226/12272/11-HH00-Watson-Johnson-1-20140226.pdf


25 “Advances in computer technology and greater access to personally identifiable information (PII) via the Internet have created online marketplaces for transnational cyber criminals to share stolen information and criminal methodologies. As a result, the Secret Service has observed a marked increase in the quality, quantity, and complexity of cybercrimes targeting private industry and critical infrastructure.” Remarks by Secretary of Defense Leon E. Panetta to the Business Executives for National Security (Oct. 11, 2012), available at http://www.defense.gov/transcripts/ transcript.aspx?transcriptid=10363 (I’ve understood that the CIA and now Secretary of Defense, I have understood that cyber attacks are every bit as real as the more well-known threats like terrorism, nuclear weapons proliferation and the turmoil that we see in the Middle East. And the cyber threats facing this...
country are growing.


27 JIM FINKE AND DHANYA SKABRACHAN, Target cyber breach hits 40 million payment cards at holiday peak http://www.reuters.com/article/2013/12/27/target-breach-idUSBRE9BH1GX20131227

28 Andrea Chang and Salvador Rodrigue, Snapchat becomes target of widespread cyberattack http://articles.latimes.com/2014/apr/02/business/la-fi-snapchat-breach-20140403


34 Resolution Agreements and Civil Money Penalties, available at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/

35 See Imposition of Civil Monetary Penalties - http://www.ecfr.gov/cgi-bin/text-idx?SID=d9862e24d6788ceffa0f7732d6776525&node=45:1.0.1.3.75.4&rgn=div6


37 http://phx.corporate-i-net/phoenix.zhtml?c=120730&p=irol-SECText&TEXT=aHR0cDovL2FwaS50ZW5rd2l6YXJkLmNvbS9mNzAwbmltcmVc2FwZWRocmVzc2VcMjAyMS5wbmdsNnxuYmFyIzhvMVQ2YXJ5dGlvbXMLNiJ1c3B1bWltcHJcMDQ0NDU2dTo5Nnc=


39 For example, on December 9, 2013, the Financial Stability Oversight Council held a meeting to discuss cybersecurity threats to the financial system. During that meeting, Assistant Treasury Secretary Cyrus Amir-Mokri said that “[t]heir experience over the last couple of years shows that cyber-threats to financial institutions and markets are growing in both frequency and sophistication.” See, Remarks of Assistant Secretary Cyrus Amir-Mokri on Cybersecurity at a Meeting of the Financial Stability Oversight Council (Dec. 9, 2013), available at http://www.treasury.gov/press-center/press-releases/Pages/jl2228.aspx.


41 Community Health Systems SEC 8-K http://phs.corporate-i-net/phoenix.zhtml?c=130739&p=red-sec&x irr=1458752723479&highlight=&year=2015&type=8k&secid=102073565&stmt=quarterly


In addition, in testimony before the House Financial Services Committee in 
2011, the Assistant Director of the FBI’s Cyber Division stated that the number and sophistication of malicious incidents involving financial institutions 
has increased dramatically over the past several years and offered numerous examples of such attacks, which included fraudulent monetary transfers, 
unauthorized financial transactions from compromised bank and brokerage accounts, denial of service attacks on U.S. stock exchanges, and hacking 
incidents in which confidential information was misappropriated. See, Testimony of Gordon M. Snow, Assistant Director, Cyber Division, FBI, U.S. 
Department of Justice, before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit (Sept. 14, 2011), 


50 ISO/IEC 15504 Information technology – Process assessment, also known as SPICE (Software Process Improvement and Capability Determination), is a 

51 This “diagnostic tool” is the first step in a “Business and Information Privacy, Security & Compliance Program Alignment Review”. By surveying a 
broad cross-section of business leaders, security, privacy and compliance leaders, and their respective staff, you will develop a better understanding 