THE FINANCIAL IMPACT OF BREACHED PROTECTED HEALTH INFORMATION

A Business Case for Enhanced PHI Security
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acknowledgments</td>
<td>5</td>
</tr>
<tr>
<td>Executive Summary</td>
<td>9</td>
</tr>
<tr>
<td>Introduction</td>
<td>11</td>
</tr>
<tr>
<td>Chapter 1 The Progression of the Health Care Ecosystem</td>
<td>13</td>
</tr>
<tr>
<td>Chapter 2 The Evolution of Laws, Rules, and Regulations</td>
<td>17</td>
</tr>
<tr>
<td>Chapter 3 PHI Data Breach Landscape</td>
<td>21</td>
</tr>
<tr>
<td>Chapter 4 Threats and Vulnerabilities</td>
<td>25</td>
</tr>
<tr>
<td>Chapter 5 Safeguards and Controls</td>
<td>31</td>
</tr>
<tr>
<td>Chapter 6 Survey Findings on Current Practices and Attitudes</td>
<td>35</td>
</tr>
<tr>
<td>Chapter 7 PHIve – The 5-Step Method of Data Breach Costing</td>
<td>39</td>
</tr>
<tr>
<td>Chapter 8 Calculating the Costs of a PHI Breach Using PHIve</td>
<td>45</td>
</tr>
<tr>
<td>Finale</td>
<td>59</td>
</tr>
<tr>
<td>Endnotes</td>
<td>61</td>
</tr>
</tbody>
</table>

Appendices – Available on the PHI project website at [webstore.ansi.org/phi](http://webstore.ansi.org/phi)

- Appendix A – Glossary of Terms and Acronyms
- Appendix B – Legal and Regulatory Liabilities
- Appendix C – Legal Considerations with Respect to Cloud Computing
- Appendix D – PHI Threat Scenarios
- Appendix E – Complete Results of Survey: Current Practices and Attitudes
The following professionals are acknowledged for their contributions to the development of this report through participation in project meetings and teleconferences.

The report was developed based on their collective inputs, following a consensus process, and does not necessarily reflect the views of the companies and organizations listed.

ActiveHealth Management

Aeritae Consulting Group, Ltd.

Affinion Security Center

Alvarez & Marsal

American Health Information Management Association

American National Standards Institute

Androscoggin Home Care & Hospice

AWARE Software, Inc.

B System Compliant, LLC

Bayhealth Medical Center

BKD LLP

Blue Cross Blue Shield of Michigan

Bluewater International

Booz Allen Hamilton Inc.

Catholic Health Initiatives

The Center for Identity Management and Information Protection at Utica College

Church Pension Group Services Corp.

Clearwater Compliance LLC

CyberRisk Partners

Deluxe Corporation

Direct Computer Resources, Inc.

DriveSavers Data Recovery, Inc.

eLCHEMY, Inc.

Manomohan Kalathil

Rob Ramer

Christine El Eris*

Mandar Rege

Harry Rhodes

Jim McCabe, Liz Neiman, Sally Seitz

Julie Porter

Dr. James Zaiss

Rustom Bhopti

Bonnie R. Millman

Matthew Lathrom

Dawn Geisert

Dr. Gary R. Gordon*

Debbie Wolf,* Ilene Yarnoff

Carrie Harding

Dr. Don Rebovich,* Ingrid Norris, Barb Stack

Stephen Tihor

Bob Chaput, Mary Chaput, Eric Lombardo, Jon Stone

Alfred Bartkiewicz

Linnea Solem*

Ed Stull*

Lynda Martel*

Erin E. Kenneally
Summit Security Group, LLC        Dan Briley
Swarmology Inc                   Malcolm Bohm
Symantec                         Axel Wirth
Terra Verde Services             Don Turnblade
Triad Biometrics LLC             Scott Coby
Trinity Mother Frances Hospitals and Clinics Patrick Leech
Tunitas Group                    Bill Pankey
University of California         Grace Crickette
University of Kansas             Jane M. Rosenthal
University of Texas Center for Identity Dr. Suzanne Barber
Veriphyr                         Nicole Borner
Wells Fargo Insurance Services, Inc. Tim McClung
Wentworth-Douglass Hospital      Peter Lincoln
West Virginia Dept. of Health & Human Resources Ellen Cannon
The White Stone Group, Inc.      Gretchen S. Johnson
Zafesoft                         Sandeep Tiwari*

*Subcommittee co-chair

Thanks and acknowledgments are given for the support and participation of all the organizations that supplied experts to this initiative. Without the contributions of these individuals and their collective expertise, particularly those that chaired the various subcommittees and that participated actively, this final deliverable would not have been possible.

- Special acknowledgment and appreciation is given to Rick Kam of ID Experts for being the project chairman and co-chair of the Finale subcommittee, and to Ed Stull of Direct Computer Resources, Inc., for co-chairing the Finale subcommittee. Their leadership and dedication in helping to shape the initiative, lead its proceedings, and build consensus for the final deliverable were instrumental in reaching a successful outcome.

- Special thanks also go to Mary Chaput of Clearwater Compliance LLC for many hours spent editing the document and synthesizing the various inputs into a coherent report.

- Appreciation is given to the American National Standards Institute (ANSI), The Santa Fe Group, and the Internet Security Alliance (ISA) for the effective project management that kept this initiative on track and allowed for a successful delivery of the final publication in a timely manner, particularly from Jim McCabe, Liz Neiman, and Sally Seitz of ANSI; Catherine Allen, Robin Slade, and Kelly Wagner of The Santa Fe Group; and Larry Clinton, Joshua Magri, and Stephanie Schaffer of ISA.

- Special acknowledgment is given to Powers Pyles Sutter & Verville PC and the Consumer Electronics Association (CEA) for hosting project meetings.

- Special thanks are extended to Deluxe Corporation for printing the report.

- Appreciation is also extended to ID Experts and MacKenzie Marketing Group for their support on communications and outreach activities.
Thank you to the following outside reviewers for their insightful comments on the draft report which contributed to the final version presented here:
- Mary N. Chaney, Founder and CEO, MBS Information Security Consulting, LLC
- James H. Dykstra, Principal, Edington, Peel & Associates
- Dr. John Adams Fox, President and CEO, FFC Computer Services, Inc.
- Mathieu Gorge, Founder and CEO, VigiTrust
- Don Horn, Director of Information Security, CareFirst Blue Cross Blue Shield
- Dr. Michael Kraten, President and co-founder, Enterprise Management Corporation
- Michael Mahoney, President, Americas and Northern Europe, International SOS
- Dr. John R. Powers, past Executive Director, President’s Commission on Critical Infrastructure Protection
- Randy V. Sabett, Counsel, ZwillGen, PLLC
- Gail Scott, Washington diplomatic consultant, author, and advisor
- Thomas J. Smedinghoff, Partner, Edwards Wildman Palmer LLP
- Dr. Robert Wah, Chief Medical Officer, CSC
- Christopher Steinbach, Chairman and CEO, The Newberry Group

Thank you to Robert Gardner, New World Technology Partners, for leading the outside review effort and for providing the consolidated and insightful feedback to the project leadership.

This initiative was made possible through the generous support of the following organizations: Clearwater Compliance LLC and DriveSavers Data Recovery, Inc. (premium sponsors); Affinion Security Center; Alvarez & Marsal; BKD, LLP; Booz Allen Hamilton; The Center for Identity Management and Information Protection at Utica College; Deluxe Corporation; Direct Computer Resources, Inc.; Europ Assistance USA; ID Experts; Terra Verde Services; and ZOHO ManageEngine (partner sponsors).
EXECUTIVE SUMMARY

Health privacy has long been perceived as the right of individuals and a necessity for effective, high quality health care. Individuals are willing to disclose the most intimate details about themselves to their doctors only with the trust that their health information will remain private and secure, whether it resides in a file at their doctor’s office, on a hospital chart, or in a claims form at their insurance provider. Indeed, protecting health information privacy has been a core component of the minimum standards for the ethical practice of medicine for thousands of years.

As the health care industry moves to adopt electronic health records (EHRs), thereby creating multiple and more expansive databases in numerous locations, there is an increase in the number of people with access to protected health information (PHI), and many more opportunities for this information to be accidentally or intentionally disclosed, lost, or stolen. This new technological capability does not alter professional ethics, and indeed emboldens the resolve to protect the privacy and security of health information to preserve access to quality health care.

Daily headlines suggest that not all organizations entrusted with PHI protection are upholding their responsibility. Health information data breaches are increasing in number and in magnitude. Insufficiently trained staff are much to blame, but the fraudulent use or sale of PHI is also on the rise. Such breaches can cause significant harm, both to the individuals whose information was breached and to the organizations responsible for protecting it.

Regulations promulgated in the last few years provide incentives for an organization’s “meaningful use” of EHRs, as well as increased enforcement and penalties for non-compliance with state and federal security regulations. Unfortunately, efforts to assure the confidentiality and integrity of PHI content have not kept pace. Individuals responsible for protecting the security of PHI face a number of challenges that may inhibit their ability to meet that responsibility, including legal and regulatory complexity, as well as lack of time, resources, and leadership commitment.

This report provides information that will enable organizations in the health care sector to build a strong business case for the benefits of investing in PHI protection and turning compliance with privacy and security laws to their market advantage. The report explores the reputational, financial, legal, operational, and clinical repercussions of a PHI breach on an organization, and offers a 5-step method — PHIve (PHI Value Estimator, pronounced “five”) — for evaluating the “at risk” value of their PHI. This tool estimates the overall potential costs of a data breach to an organization, and provides a methodology for determining an appropriate level of investment to reduce the probability of a breach.
A comprehensive resource about the critical importance of safeguarding PHI, the report offers information about the stakeholders involved in the health care ecosystem; the evolution of laws, rules and regulations designed to protect PHI; the causes and increasing number of data breaches; the most common threats and vulnerabilities to the security of PHI; and safeguards and controls that organizations can put in place to mitigate the risk of a breach.

The report also includes insights on current industry practices and attitudes in relation to protecting PHI, which emanated from a survey of individuals responsible for safeguarding this important health data.

Armed with the information contained in this report, organizations operating in the health care sector can head off the potentially devastating consequences of a PHI data breach by thoughtfully investing in enhancing their privacy and security programs at a level that reduces that probability or impact.

This report is organized as follows:

- Chapter One: An overview of how the health care ecosystem has expanded in recent years to include more organizations, all with the responsibility for the protection of PHI.
- Chapter Two: A comprehensive summary of how the laws and regulations that impact PHI protection have evolved since the enactment of HIPAA, the Health Insurance Portability and Accountability Act of 1996, including gaps and weaknesses in those laws.
- Chapter Three: A review of some recent PHI breaches – what happened and how – along with a discussion of the value of PHI.
- Chapter Four: A discussion of the more common threats now facing all organizations in the health care ecosystem and related vulnerabilities, including a case study of the repercussions of a PHI breach.
- Chapter Five: Highlights of the interaction and effectiveness of certain safeguards and controls related to policies, procedures, and technology to mitigate the risk of a PHI breach.
- Chapter Six: Insights from a survey on what is being done to secure PHI, what is not, and why.
- Chapter Seven: A description of PHIve, a 5-step method for assessing an organization’s security risks, identifying gaps, and calculating the potential costs of a PHI breach.
- Chapter Eight: A demonstration of how PHIve works to estimate the financial costs of a PHI breach in terms of reputational, financial, legal, operational, and clinical repercussions. A detailed example of costing a PHI breach is given, including calculations and suggestions, and highlighting relevance and impact considerations.

The chapters are supplemented by a number of online appendices, hyperlinked to this report, which contain research notes from the various project subcommittees.
The hope, and expectation, has been that driving health care entities to adopt electronic health records (EHRs) would reduce medical costs, provide for accessibility to health care information, and increase the quality of care. But the potential benefits of EHRs have been accompanied by an increase in the number of organizations handling protected health information (PHI) and, consequently, a rapidly growing volume of electronic health care data breaches.

Some of this can be attributed to insufficient training of staff and insufficient attention to preventive security measures. However, the substantial financial rewards for stolen health records also have grown, along with the ability of criminals to crack the security mechanisms designed to protect PHI.

Complicating matters is the fact that requirements for PHI protection have expanded beyond traditional provider and billing organizations involved in carrying out treatment, payment, or health care operations (covered entities) to include an increasing number of organizations supporting those covered entities in the handling of PHI (business associates). Many other organizations that are handling PHI today may not fit the regulatory definition of covered entities or their business associates, such as health exchanges, data miners, law firms, and other subcontractors. These participants in the health care ecosystem may not understand the requirements or the importance of protecting PHI.

Preventive measures such as security technology, policies, and procedures to protect PHI can be implemented to help mitigate risk and reduce either the probability or the impact of a PHI breach. Such measures may position an organization to improve care, strengthen its reputation, and benefit from operational efficiencies that can come from adopting EHRs. Without such safeguards, data breaches will continue to erode the public’s confidence in the health care system and the expectation that the privacy of their health information will be protected.

So why have organizations not already fully implemented these preventive measures? A survey of participants in the health care industry, conducted in conjunction with the development of this report, provides insights into the challenges organizations face in strengthening their compliance programs. Despite a sense of having “effective policies” and taking “effective steps” toward compliance, respondents note a lack of both resources and leadership support as barriers to “ensuring requirements are currently being met.”
But if healthcare industry leaders really understood the privacy expectations of their patients and customers and the repercussions and costs resulting from a PHI breach, as well as the advantages that increased security and HIPAA compliance could bring to their organizations, the return on investment (ROI) in strengthening their compliance programs would be far more attractive.

In fact, privacy and security programs would likely become a high priority if the health care industry more widely understood the increasing costs of class action lawsuits resulting from data breaches, not to mention the statistical probability that nearly all health organizations will experience an electronic data breach in the next few years.

To understand the value of PHI in an organization’s care is to understand what is lost if that PHI is breached. This report provides a framework for calculating the cost of a data breach for any organization responsible for protecting PHI, thereby making a convincing case that achieving HIPAA compliance and data security is one of the best investments an organization can make.

The threats are real and ubiquitous, the risks are high, and the financial, reputational, and legal repercussions to individuals and organizations can be severe.

A Note about Terms before Getting Started

For purposes of this report, a shorthand definition of protected health information (PHI) is individually identifiable health information protected by any federal, state, or local law, rule, or regulation. Electronic protected health information (ePHI) would be PHI that is created, stored, or accessed through electronic means. Also, the terms “breach,” “data breach,” “privacy breach,” “security breach,” and “PHI breach” are used liberally and interchangeably within this report to describe the unauthorized disclosure of information that compromises the availability, integrity, or confidentiality of PHI.

It is recognized that there are other data beyond PHI that may simultaneously be breached that give rise to legal liability. Statutory and regulatory definitions are listed in Appendix A – Glossary of Terms and Acronyms.
CHAPTER ONE

The Progression of the Health Care Ecosystem

When the HIPAA Privacy statute was first enacted in 1996, most health information was on paper. In fact, even by 2006, according to a report from the Centers for Disease Control and Prevention (CDC) (see Figure 1 below), the use of electronic medical records (EMRs – the digital record of medical and treatment history of the patients in one practice) among office-based physicians in the U.S. stood at 29.2%. Only 12.4% of physicians used EMR systems with all four of the features considered necessary for a minimally functional system – systems allowing for computerized orders for prescriptions, computerized orders for tests, electronic viewing of test results, and electronic viewing of clinical notes.

Thanks to incentives for adoption and penalties for non-adoption under the Medicare and Medicaid programs, the use of EMRs grew significantly over time. By 2008, still only 41.5% of office-based physicians reported using any EMR system, but that is more than double the number in 2001.¹

Figure 1: Percentage of office-based physicians with electronic medical record (EMR) systems: United States, 2001 - 2008

Notes: Any EMR is a medical record system that is either all or partially electronic (excluding systems solely for billing). Fully functional systems are a subset of basic systems. Excludes radiologists, anesthesiologists, and pathologists.

Source: CDC/NCHS, National Ambulatory Medical Care Survey

¹ The Financial Impact of Breached Protected Health Information

download this publication freely at webstore.ansi.org/phi

The Health Care Ecosystem 2012

The health care ecosystem is the arena in which health care services take place, comprised of individuals, providers, clinical support, payers, and others, including those that support the physical and electronic infrastructures, in addition to the information that is shared and that flows between them.

With the growth of electronic health records (EHRs – the evolution of EMRs to be more focused on the total health of the patient and designed to be shared with other health care providers), there has been a surge in the number of organizations that are now stakeholders in the health care ecosystem (see Table 1). These include new points of care (e.g., urgent care facilities, clinicians in retail stores, virtual offices associated with telemedicine delivered over the Internet), new business associates (e.g., revenue cycle companies, collections agencies), and organizations offering a myriad of electronic and web-based support services (e.g., data transmission, software-as-a-service and cloud computing, mobile devices, web portals).

These stakeholders are responsible for the confidentiality, integrity, and availability of all PHI they create, receive, maintain, transmit, or store. This responsibility includes implementing appropriate safeguards against any reasonably anticipated threats or hazards to the security or integrity of that information. They must ensure:

- **Confidentiality**: data or information is not made available or disclosed to unauthorized persons or processes;
- **Integrity**: data or information has not been altered or destroyed in an unauthorized manner; and
- **Availability**: data or information is accessible and useable upon demand by an authorized person.

### Table 1: Stakeholders in the Health Care Ecosystem

<table>
<thead>
<tr>
<th>Points of Care</th>
<th>Payers</th>
<th>Clinical Support</th>
<th>Business Associates</th>
<th>Others</th>
<th>IT Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Primary care physicians&lt;br&gt;- Secondary physicians&lt;br&gt;- OB/GYN physicians&lt;br&gt;- Clinics&lt;br&gt;- Hospitals&lt;br&gt;- Therapists&lt;br&gt;- Homeopaths&lt;br&gt;- Long term care facilities&lt;br&gt;- Rehab facilities&lt;br&gt;- Assisted living&lt;br&gt;- Urgent care facilities&lt;br&gt;- Telehealth/telemedicine&lt;br&gt;- Retail physicians</td>
<td>- Primary insurers&lt;br&gt;- Secondary insurers&lt;br&gt;- Medicare&lt;br&gt;- Medicaid&lt;br&gt;- Employers: benefits administrators&lt;br&gt;- Consumers</td>
<td>- Clinical labs&lt;br&gt;- Research labs&lt;br&gt;- Imaging companies&lt;br&gt;- Pharmacies&lt;br&gt;- Mail-order pharmacies&lt;br&gt;- Phlebotomists</td>
<td>- Pharmacy benefits managers&lt;br&gt;- Third-party administrators&lt;br&gt;- Benefits administrators&lt;br&gt;- Claims review/utilization&lt;br&gt;- Billing processors&lt;br&gt;- Revenue cycle companies&lt;br&gt;- Payment agencies&lt;br&gt;- Collection agencies&lt;br&gt;- Hospital discharge care support&lt;br&gt;- Disease management companies&lt;br&gt;- Wellness companies&lt;br&gt;- Fulfillment companies&lt;br&gt;- Health risk assessment organizations</td>
<td>- Life insurance companies&lt;br&gt;- Law firms&lt;br&gt;- Consultants&lt;br&gt;- Auditors&lt;br&gt;- Accreditation firms&lt;br&gt;- Application trouble-shooters&lt;br&gt;- Pharmaceutical/medical device companies&lt;br&gt;- Contract research organizations</td>
<td>- Data transmission (HIE)&lt;br&gt;- Data storage&lt;br&gt;- Data back-up&lt;br&gt;- Data recovery services&lt;br&gt;- Software as a service (SaaS) offerings&lt;br&gt;- On-line diagnostic services&lt;br&gt;- Mobile devices&lt;br&gt;- Web portals: physicians&lt;br&gt;- Web portals: consumers</td>
</tr>
</tbody>
</table>
The Ramifications

Electronic health information systems have become a “game changer” in the threat to health information privacy. In addition to the increase in the number of organizations that handle PHI and the increase in the financial incentives for medical identity theft, the frequency and the size of unauthorized PHI disclosures have continued to increase, along with the costs to the organizations unfortunate enough to have suffered such breaches.²

In the 15 years since the enactment of HIPAA, it has become evident that electronic health information technology offers the potential for future significant benefits, but it also has opened up the PHI universe to an increasing number of threats to the privacy and trust on which the health care delivery system is based. For the first time in the history of medicine, it is possible to:

- Improperly disclose identifiable electronic health information of millions of individuals “in a matter of seconds;”³
- Steal health information without having physical access to it and from locations that may be beyond the reach of U.S. laws;⁴ and,
- Breach an individual’s PHI in a manner that makes it impossible to restore.⁵

The threats to the security of PHI are not specific to one stakeholder group but are ubiquitous throughout the entire ecosystem due to the volume and availability of PHI data and transmission of electronic PHI records (ePHI). As depicted in Figure 2, the interrelationship of the stakeholders, the information flows of PHI, and the vulnerability/risk points indicate that the information is at risk whether in motion or at rest. At each instance, a copy of the data is created resulting in its residing in multiple databases and thereby providing greater vulnerability to threats.

Any organization or person that creates, handles, transmits, or stores PHI (“PHI protector”), regardless of size or function, is a member of this health care ecosystem and is responsible for the safeguarding of the PHI entrusted to its care, all under the watchful eye of legal and regulatory agencies.

The White House has recognized that the growing use of online transactions generally has increased “online fraud and identity theft,” which “cost companies and individuals billions of dollars each year” and often “leave in their wake a mess of ruined credit and damaged finances that can take years to repair.”

In addition, “[t]he potential for fraud and weakness of privacy protections often leave individuals, businesses, and government reluctant to conduct major transactions online.”⁶ While the total potential cost and liability due to electronic fraud and privacy breaches has been difficult to quantify with precision, the White House has concluded that “the problem is real and it is increasing.”⁷
The damage and liability that can result from electronic health information fraud and privacy violations are particularly acute. A stolen Social Security or credit card number can be replaced, but information about one’s health status, once stolen, can be copied, altered, and circulated repeatedly. So the potential damage from a PHI breach to the individual and the payer is essentially unlimited.

As more individuals have become the victims of health information privacy breaches, public concern has grown, members of Congress have become involved,8 state and federal laws protecting health information privacy have multiplied, enforcement of those laws has ramped up, and potential legal liability for violations of privacy laws has increased.

This growing risk of health information privacy liability is occurring at a time when there is significant pressure to reduce spending on health care.9 In addition, the ability to protect health information has not matched the public’s expectations for privacy, to the detriment of the finances and reputations of organizations in the health care ecosystem.

If PHI is not adequately safeguarded, the vision of a truly interoperable electronic health information system in the United States could be in jeopardy, just as it was a significant issue that contributed to Britain’s decision to abandon its plans for a centralized electronic health information system.10
Management and reduction of the financial and business liability arising from mishandling PHI is only possible with a clear understanding of, first, the privacy rights of patients and customers, and, second, the requirements and enforcement mechanisms of health information privacy laws and professional ethics. In other words, enterprises that handle health information must be aware of consumer privacy rights and expectations in order to meet them.

The public’s perception and expectation of a right to health information privacy is rooted in standards of professional ethics, has been read into (or some would say is “found within the ‘penumbra’ of”) the U.S. Constitution, and is recognized in each state’s tort law. Accordingly, a PHI protector must be cognizant of these expectations and how they influence the regulatory environment.

The Supreme Court has repeatedly recognized that individuals have a right to informational privacy that is protected from government violation by one or more sections of the Constitution and that, whatever its scope, the right appears to encompass health care information.\textsuperscript{11} According to the Court, the right to privacy is “older than the Bill of Rights – older than our political parties, older than our school system.”\textsuperscript{12} The Constitutional privacy protection is strongest where the individual has a “reasonable expectation of privacy” in the health information arising from his or her personal health care.\textsuperscript{13} Generally, “the more intimate or personal the information, the more justified is the expectation that it will not be subject to public scrutiny.”\textsuperscript{14} Information about mental health treatment, sexual orientation and conditions, physical defects or disabilities, or other clinical treatment detail is typically viewed by courts as more intimate and personal.

While the Constitution only protects an individual’s right to informational privacy against federal and state governments, this right creates an expectation that the individual has a more general right to privacy, which is, in fact, protected by other laws. States, too, have recognized an individual’s right to privacy, holding individuals and organizations accountable for breaches of privacy under various tort law theories and pursuant to state statutes. Many of the headline-grabbing financial settlements related to privacy breaches stem from lawsuits based on state tort law.

A constitutionally based right to privacy for sensitive personal information has also been recognized by the other two branches of the federal government – Congress, and the Executive Branch through the U.S. Department of Health and Human Services (HHS).

According to Congressional findings, Americans expect a right to privacy for personal information about themselves that is a “personal and fundamental right protected by the Constitution of the United States.”\textsuperscript{15} HHS has determined that “privacy
is necessary to secure effective, high quality health care." Further, in the HIPAA Privacy rulemaking, the right to privacy of highly personal information is a “fundamental right” of all Americans” and “one of the key values on which our society is built.”

Although protection requirements for PHI evolved slowly at first, in recent years they have expanded dramatically as EHRs have been more widely adopted. When HIPAA was enacted in 1996, only covered entities were subject to established standards for the privacy and security of PHI. Since then:

- Detailed HIPAA Privacy and Security regulations were issued, subjecting only certain “covered entities” to both privacy and security standards;
- The Genetic Information Non-Discrimination Act of 2008 has been enacted, affording special privacy protections for genetic information; and
- The American Recovery and Reinvestment Act of 2009 was passed, which included:
  - incentives for health care providers and practitioners to adopt EHRs, and
  - the Health Information Technology for Economic and Clinical Health (HITECH) Act that enhanced the health information privacy rights of individuals, and the penalties for those who violate those rights, and extended HIPAA privacy and security standards (and penalties) for ePHI to “business associates” of covered entities.

### Table 2: A summary of the HIPAA laws, rules, and regulations

<table>
<thead>
<tr>
<th>1996 HIPAA Subtitle F:</th>
</tr>
</thead>
<tbody>
<tr>
<td>HHS secretary is required to establish standards for the privacy and security of PHI held by covered entities (CEs).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Defined requirements for the protection of individually identifiable health information held by covered entities (protected health information or “PHI”) and gives individuals specific rights with respect to that information</td>
</tr>
</tbody>
</table>

#### Requirements of covered entities:
- May not use or disclose PHI except as permitted or required by the Privacy Rule
- 2005: Established obligations of business associates (BA)
  - Required CE to obtain contractual and satisfactory assurances that the BA will safeguard PHI
  - Established permitted and required uses and disclosures, return, and/or destruction for BA
  - Authorized termination of contract by CE if BA violated material term of contract

#### Rights of individuals:
- Be informed of CE privacy practices and privacy rights
- Obtain a copy of their medical records
- Amend incomplete or incorrect health information
- Learn of certain disclosures of their PHI made by a CE or BA
- Applies to all forms of PHI (electronic, written, or oral)

### 2003 – 2010 HHS Office for Civil Rights (OCR) Privacy Rule Compliance Investigations

- Most common types of CEs required to take corrective action (in order of frequency):
  - Private practices
  - General hospitals
  - Outpatient facilities
  - Health plans
  - Pharmacies

- Issues investigated most by OCR (in order of frequency):
  - Impermissible uses and disclosures of PHI
  - Lack of safeguards of PHI
  - Denial of individuals’ access to their PHI
  - Uses or disclosures of more than the minimum necessary PHI
  - The inability of individuals to file complaints with CEs
### 2003 HIPAA Security Rule (45 CFR 160 and Subparts A and C of Part 164)

Established national standards to protect electronic PHI created, received, used, or maintained by a covered entity

#### Requirements of covered entities:
- Requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of electronic PHI
- Required to be in compliance with the Security Rule by April 20, 2005

#### Enforcement authority:
- July 27, 2009 – present: HHS transferred authority to OCR

### 2005 – 2010 OCR Security Rule Compliance Investigations

Issues investigated most by OCR (in order of frequency):
- Failure to demonstrate adequate policies and procedures or safeguards to address response and reporting of security incidents
- Security awareness and training
- Access controls
- Information access management
- Work station security

### 2009 HITECH Amends HIPAA (Title XIII of Division A and Title IV of Division B of ARRA)

Provides incentives to providers to allow for implementation and utilization of electronic health records

#### Meaningful use:
- Provision is made for incentive payments to eligible professionals (EPs), eligible hospitals, and critical access hospitals (CAHs) who participate in the Medicare and Medicaid programs and who adopt and successfully demonstrate the meaningful use of certified electronic health records (EHRs)

#### Details of incentives:
- Federal incentive payments available to doctors and hospitals upon:
  - Adoption of EHRs and
  - Demonstration of improvements in quality, safety, and effectiveness of care
- Medicare: if eligible, up to $44,000 over 5 years
- Medicaid: if eligible, up to $63,750 over 6 years
  - 1st year: for adopting, implementing, and upgrading certified EHR technology
  - Subsequent years: for demonstrating meaningful use
It can be expected that additional regulations will come and more entities will be held responsible, as the existing laws are, in many cases, non-specific or conflicting, and leave gaps in responsibility. For example:

- The HIPAA Privacy and Security Rules only apply to “covered entities” and their “business associates,” but health information is handled by many other individuals and entities, including subcontractors to business associates.

- The Data Breach Notification Rule does not specify breach notification requirements for data breaches caused by researchers, law officials, or those who subpoena records.

- The Privacy Rule requires covered entities to inform individuals “in plain language” of their health information privacy rights but does not list the right to health information privacy among those rights.

- The HIPAA Privacy and Security Rules and the “Privacy” section of the HITECH Act contain definitions of key terms but do not define “health information privacy.”

- The HIPAA Privacy Rule provides that covered entities and their business associates may use and disclose an individual’s identifiable health information without consent (even over the individual’s objection) for treatment, payment, and health care operations, but standards of professional ethics, which HHS says “retain their vitality,” have traditionally prohibited such disclosures with narrow exceptions.

A former head of HHS’s Office of Health Information Technology stated that “HIPAA makes no sense” in the current environment because it did not anticipate that health information would pass through many hands.

More information is available in Appendix B – Legal and Regulatory Liabilities.
CHAPTER THREE

The number of Americans that have become victims of health information privacy breaches has grown rapidly with the adoption of EHRs.

- Between 2005 and 2008, nearly 230 million electronic records were breached including almost 39.5 million electronic health records.24

- In the past two years, the health information privacy of nearly 18 million Americans has been breached electronically, which is “equivalent to the population of Florida.”25

- In the period September through November of 2011:
  - A government benefits program suffered the theft of electronic health records of 4.9 million military personnel;26
  - A reputable West Coast health care system experienced the electronic theft of health information for 4 million of its patients;27 and
  - A major academic medical center inadvertently disclosed the electronic health records of 20,000 of its patients.28

- In a November 2011 survey completed by 72 provider organizations conducted by Ponemon Institute, 96% reported having had at least one data breach in the past 24 months. On average, health organizations have had four data breach incidents during the past two years. Compared to the prior year, there were increases in both the frequency of data breaches (up 32%) and the average economic impact of a breach (up 10%). The average number of lost or stolen records per breach also increased (2,575 compared to 1,769 the year before). In addition, there was a 26% increase in respondents who said their data breaches led to cases of identity theft. Notable was the percentage of organizations fully implementing or in the process of implementing an electronic health records system, which increased from 56% last year to 66% in this year’s study.29

Health information privacy violations that in the past typically involved lost or misplaced information increasingly involve medical identity theft by organized crime that is difficult to detect and correct.30 According to 2010 reported data collected by the Identity Theft Resource Center, data breaches are occurring in health care at nearly three times the rate as in banking and finance.31 This may be due to more intense reporting requirements in health care, the greater number of people who have access to health data, and the growing black market for patient medical information.32

While the reason for stealing medical records may be baffling to some, it certainly is not to those who are profiting from those illegal activities.
Fraud resulting from medical identity theft primarily takes two forms: (1) physician identification numbers that are stolen and used to bill for services, and (2) patient identification information that is stolen (or lent to friends and relatives) and used to obtain services or to bill for services.\(^{33}\)

In a survey of 600 executives from hospitals, physician groups, health insurance companies, and pharmaceutical and life sciences companies, PricewaterhouseCoopers (PwC) found that 36% of the surveyed hospitals and physician groups said patients had sought services using somebody else’s name and identification.\(^{34}\)

At approximately $60 billion per year, Medicare fraud has become “one of, if not the most profitable, crimes in America.” In south Florida, Medicare fraud has replaced cocaine as the major criminal enterprise.\(^{35}\)

Further evidence of the scope and implications of clinical fraud is gleaned from early fraud analysis, which has led to estimates of emergency department, emergency services clinic, and hospital inpatient clinical fraud rates of between 2-10\% of all patients treated. That analysis revealed that the majority of clinical fraud is perpetrated in an effort to obtain prescription narcotics for illegitimate use, but up to 5\% of clinical fraud appears to be perpetrated for receipt of free health care. In both scenarios, the impact on the PHI breach victim whose information is used to commit clinical fraud comes in the form of monetary loss, possible inability to obtain or retain insurance, and corruption of medical history. Damage done to the victim can eventually impact the facility where the breach occurred as the victim seeks reimbursement or sues for damages.\(^{36}\)

**Put It This Way**

- A thief downloading and stealing data can get $50 on the street for a medical identification number compared to just $1 for a Social Security number. For those receiving the medical ID number and using it to defraud a health care organization, the average payout is more than $20,000, according to Pam Dixon, executive director of the World Privacy Forum. Compare that to just $2,000 for the average payout for regular ID theft.\(^{37}\)

- A clerk in a medical clinic in a Florida hospital stole the medical IDs of 1,100 patients and sold them. The numbers were subsequently used to bill Medicare for $2.8 million in false claims.\(^{38}\)

- A hospital in Orlando, Florida, fired three employees for improperly reviewing emergency department records of 2,252 patients, reportedly to forward information about accident victims to lawyers.\(^{39}\)

**What about Snooping?**

In a 2011 survey conducted by Cyber-Ark of 1,422 IT staff and C-level professionals across North America, Europe, the Middle East, and Africa (EMEA), 28\% of North American IT staff respondents admitted to snooping while 44\% of EMEA IT staff admitted the same.\(^{40}\) In a patient privacy breach study of compliance and privacy officers at mid-to-large-size hospitals and health care service providers, Veriphyr, a vendor of data analytics software that generates access activity logs of patients’ medical records, found that 35\% of studied breaches “involved snooping into medical records of co-workers and 27\% involved viewing records of friends and relatives.”\(^{41}\) And when it comes to the medical records of celebrities?

- The *Los Angeles Times* reported that hospital officials from UCLA Medical Center fired a member of its staff who reviewed a prominent celebrity’s records without authorization.\(^{42}\) The employee was paid $4,600 by the *National Enquirer*.\(^{43}\)
The Arizona Star reported that the University Medical Center in Tucson, where Representative Gabrielle Giffords was taken following the shooting rampage that left her injured, fired three employees for allegedly accessing confidential medical records inappropriately.\textsuperscript{44}

How Do People Feel about Breaches?

Not surprisingly, the frequent reports of massive breaches of electronic health information have eroded the public’s confidence in the ability of health care providers and organizations to protect the privacy of PHI. Approximately 69% of Americans have heard of, or read of, health records being stolen from health care providers.\textsuperscript{45} A majority of Americans (54%) only trust their health care providers “somewhat” to protect the privacy of their health care information, and nearly 60% believe that their medical records are not adequately protected by existing laws.\textsuperscript{46}

The National Committee on Vital and Health Statistics – designated by HIPAA to provide advice on implementation – found after months of hearings that “public trust is lacking,” and that the benefits of electronic health information are unlikely to convince individuals to take the personal risk of making their health information available over a National Health Information Network.\textsuperscript{47} HHS findings confirm that Americans believe they have a right to privacy for their health information and that it should be protected as the nation moves toward adopting electronic health information technology.\textsuperscript{48} An online poll of 2,000 adults revealed that 97% of the public believe health care providers and insurers should not be able to share their health information without their consent.\textsuperscript{49} According to HHS, the lack of public confidence in health information privacy protection will drive up the cost of health care.

In the beginning, HHS estimated that the HIPAA Privacy Rule would add $18 billion to health care costs over the period 2003 through 2013.\textsuperscript{50} However, HHS assumed that much of this cost would be offset by the savings that would be achieved if people were more willing to obtain preventive health care and treatment due to their belief that “their information will be used properly and not disseminated beyond certain bounds without their knowledge and consent.”\textsuperscript{51} For example, HHS has found that nearly $800,000 could be saved annually by convincing the more than two million Americans who fail to seek treatment for mental illness due to privacy concerns to seek needed treatment.\textsuperscript{52} Hundreds of millions of dollars more could be saved annually by adopting privacy measures that would encourage those with HIV/AIDS and other sexually transmitted diseases to seek diagnosis and treatment.\textsuperscript{53} Those anticipated savings will not be achieved unless the public believes the privacy of their health information will be protected in electronic health information systems.

On the Horizon

The White House has outlined a national strategy for addressing the growing fraud and privacy problems with electronic information systems that has as its guiding principle “[t]he enhancement of privacy and support of civil liberties.”\textsuperscript{54} That strategy calls for adopting electronic identity solutions that are privacy-enhancing, secure, resilient, interoperable, cost-effective, and easy to use.\textsuperscript{55} The strategy will take “many years” to develop and will require the “dedicated efforts of both the public and private sectors.”\textsuperscript{56} So it is unclear whether the schedule for implementing such a strategy is consistent with the goal in the HITECH sections of the American Recovery and Reinvestment Act of 2009 to achieve widespread adoption and meaningful use of electronic health records by 2014.\textsuperscript{57}

In summary, the right to health care privacy exists and the organizations that handle PHI are legally and ethically responsible for protecting it. There are bad-intentioned people who are focused on stealing that data, as well as good but untrained people who are not aware of their responsibilities and the means of protection.
The balance of this report will help PHI protectors to:

1. Provide suggested safeguards and controls to protect against threats and related vulnerabilities.
2. Recommend a scale for determining “unacceptable” levels of risks.
3. Identify the sources and range of financial costs, reputational harm, and legal liabilities that can arise from violations of the expectation and trust that PHI will be protected.
4. Provide a tool for quantifying the financial impact to the organization should a breach occur.
5. Build a robust business case for investing in enhanced PHI security.
CHAPTER FOUR

Eleven Elements That Threaten the Security of PHI

While security threats and vulnerabilities to the confidentiality and integrity of PHI are well documented and are generally independent of what part an organization plays within the health care ecosystem, an analysis of the most recent data breaches highlights the following major contributors:

Figure 3: Top 11 elements threatening PHI security

- The “Insider” is a current or former workforce member (employee, contractor, or temporary staff) who is known as a **Malicious Insider** (1) or a **Non-Malicious Insider** (2), depending upon intent. The non-malicious insider is typically an authorized user who causes the accidental disclosure of PHI due to human error or lack of training. The malicious insider is intent on breaching security controls to gain access to or manipulate PHI in order to harm or disrupt the organization or for personal gain. According to Verizon’s 2010 Data Breach Investigations Report, almost half (48%) of all data breaches involve the participation of an insider, but only 10% are unintentional – whereas 90% are deliberate and malicious and usually involve misuse of privileges. Of the crimes tied to insiders, almost one-quarter (24%)
Almost half (48%) of all data breaches involve the participation of an insider, but only 10% are unintentional – whereas 90% are deliberate.

were perpetrated by employees involved in a job change, such as those newly hired, the recently promoted, or those being fired or resigning. Insiders can be the most dangerous of attackers as they are usually familiar with organizational policies, procedures, authorization codes, file systems, and system access, and they are most likely to know how to cause the most damage.

The Outsider (3) is a non-workforce-member who is intent on disrupting the organization or gaining access to PHI for nefarious purposes. The outsider threat can use many techniques to gain access to PHI, including computer viruses, Trojan horses, worms, social engineering, IP spoofing, mail bombing, password cracking, or packet replay or modification, among other methods. The “hacktivist” group Anonymous recently focused their efforts on a computer crimes investigator, hacking into his emails, voicemails, and SMS text messages, posting 38,000 emails containing “computer forensics techniques, investigation protocols as well as highly embarrassing personal information.”

Some of most significant breaches in terms of number of records lost are caused by Lost/Stolen Media (4). The typical example is a lost backup tape or a stolen laptop. Findings in a PwC survey indicated that “theft accounted for 66% of reported health data breaches in the past two years.” Recently, a thief stole medical information of more than four million patients of Sacramento-based Sutter Health by the simple act of breaking a window with a rock and stealing a desktop computer at the affiliated Sutter Medical Foundation.

Many breaches occurring in the health care ecosystem are caused during the Dissemination of Data (5) between stakeholders of the ecosystem. This involves the use of technologies with weak controls, such as FTP (file transfer protocol) sites, which lack the security, tracking, and auditing capabilities of sFTP (secure file transfer protocol) to ensure the protection of health information. “Drug development data, clinical trial data, health records, billing information, X-rays, MRIs, and social security numbers are some of the types of highly sensitive data that are at risk of exposure simply because they are being exchanged frequently among multiple third parties.” Organizations involved in the transmission of data must invest in technology and processes that protect the data in transit and at rest, while providing the ability to manage and audit data transfers between business partners, service providers, and customers.

As the size and price of portable electronic communication devices continue to decrease, we now find that many health care staff have access to PHI using Mobile Devices (6) (e.g., PDAs, iPads, flash memory cards, etc.). These devices do not have the mature security controls commonly found in computer systems. Between September 22, 2009, and May 8, 2011, mobile devices were responsible for 116 breaches, exposing the PHI of more than 1.9 million patients. According to a recent Manhattan Research study, “64% of physicians own smartphones and 30% of physicians have an iPad, with another 28% planning to buy one within six months. Ten thousand mobile health care applications are available today on the iPad, with a larger [sic] number of them created to provide access to electronic health records. Additionally, one-third of physicians use their mobile devices to input to EHRs while seeing patients, while the information is fresh.” In the November 2011 Ponemon study, 81% of participants reported the use of mobile devices to collect, store, and/or transmit some form of PHI, yet 49% admitted their organizations do nothing to protect these devices. Similarly, 55% of those participating in the previously cited PwC survey said that privacy and security issues associated with mobile technology had not yet been addressed.

Outsourcing has grown exponentially over the past fifteen years and is common within the health care ecosystem. Business Associates, Suppliers, Vendors, and Partners (7) are subject to exactly the same threats as the health care provider. The contract or other arrangement between a covered entity and business associate must provide that the business associate will use appropriate safeguards to prevent use or disclosure of PHI and establish permitted and required uses and disclosures, among other requirements. Not only were business associates involved in more than 20% of all PHI data breaches, the top-three breaches in terms of the number of individuals affected involved BAs and represented more than 45% of all individuals that have been reported to HHS as being affected – TRICARE, 4.9 million

Almost half (48%) of all data breaches involve the participation of an insider, but only 10% are unintentional – whereas 90% are deliberate.
affected, September 2011; Health Net, 1.9 million affected, January 2011; and New York City Hospitals Corp., 1.7 million affected, December 2010. And yet, only 36% of health organizations perform a pre-contract assessment of their business associates, and only about 25% conduct post-contract compliance assessments.69

As providers of storage and transmission services for PHI, Cloud Providers (8) must protect against the multiple opportunities for physical and electronic breaches. The ascent and prominence of this newest generation of outsourcing services used by organizations in the health care ecosystem has resulted in a potential increase in risk to the security of PHI data. That risk comes from a number of security vulnerabilities:

- Hacking from publicly available interfaces to the network;
- Electronic access to sensitive information stored on common servers by different organizations;
- Physical access by multiple parties, as cloud providers may have a number of storage locations; and
- Inconsistent rules for data protection and data breaches across geographic regions.70

The popularity of cloud computing is based on the cost efficiencies of outsourcing both the storage and the security compliance requirements. The widely held belief that security at a cloud computing service, uncontrolled by the covered entity, potentially can be compromised has done nothing to slow the swift adoption of cloud computing usage. The National Institute of Standards and Technology (NIST) has finalized its first set of guidelines for managing security and privacy issues in cloud computing (NIST Special Publication 800-144).71 This publication provides an overview of the challenges of public cloud computing to privacy and security, and highlights considerations when outsourcing to a public cloud environment. According to Gartner Group, cloud computing is expected to represent a $150 billion market by 2014.72 The net result of employing cloud computing services for the maintenance of PHI data has been to add another layer of potential breach exposure to a health care organization. Ultimately, the consumer of the cloud services retains full legal responsibility for compliance with any applicable statutes and regulations.

For more information, read Appendix C – Legal Considerations with Respect to Cloud Computing.

Understanding the vulnerabilities created by new technologies, as well as evolving motives, is critical for establishing appropriate safeguards to prevent disclosures of PHI. These vulnerabilities include the difficulty in providing safeguards for the Virtual Physician’s Office and Wireless Health Care Device Technology, and against State-Sponsored Cyber Crime.

- **Virtual Physician’s Office (9) and Wireless Health Care Device Technology (10):** No longer limited to a face-to-face consultation, the doctor-patient relationship has moved out of the doctor’s office or clinic and into cyberspace, bringing along with it issues related to the legal protections of physician-patient privilege and privacy, and online data protection. Email, texting, video conferencing, digital medical cameras, digital stethoscopes, diagnostic equipment, and remote monitoring are altering the traditional method of delivering medical care with real-time diagnostics and increased transmission of patient data.

Millions of Americans now rely upon the Internet as a primary source of medical information or education about their own symptoms, conditions, diagnoses, and treatments. The practice of telemedicine – consulting with another physician by using technology – is constantly evolving and expanding into areas never before imagined. Physicians are establishing their own web sites and some are now practicing medicine on the Internet. The practice of medicine has now evolved to include interactions that might not ordinarily have been considered to have the legal protections of doctor-patient privilege. These interactions are, at times, both real and virtual, and the consumer-patient is now in a situation where it is difficult to identify exactly who is the party on the other end or where their information is being sent.73
State-Sponsored Cyber Crime (11): State-sponsored cyber attacks are on the rise and the Pentagon has concluded that “computer sabotage coming from another country can constitute an act of war,” allowing the U.S. to respond using military force. Here are some examples:

- Operation “Shady Rat” breached networks of 72 organizations across the globe;
- Foreign hackers stole 24,000 sensitive files from the Pentagon in a single breach;
- “Aurora” attacks targeted Cisco, Juniper, Google, and Adobe;
- “Night Dragon” attacks targeted global oil and gas data.

Although careful not to mention any specific countries, British Foreign Secretary William Hague closed a two-day conference on cybersecurity with a warning to foreign governments that a more confrontational approach will be undertaken if state-sponsored cyber-attacks do not stop.

The following scenario is representative of a compilation of recent security breaches, along with repercussions that can follow, and preventive measures that could have been taken. According to HIPAA regulations, covered entities must ensure protections for PHI in a business associate agreement when outsourcing services to business associates, suppliers, vendors, and partners who create, receive, maintain, transmit, or store PHI. The legal responsibility for a data breach caused by a business associate belongs to the covered entity, and that, along with the resulting financial ramifications, should not be underestimated.

PHI Threat Scenario: Business Associate

In this scenario, a major New York City hospital server housing a database of over 845,000 patient records could no longer be accessed due to the mechanical failure of the hard drives. The IT manager followed procedures to restore the database from the hospital’s magnetic backup tapes, but the backup tapes were blank.

The permanent loss of the database records would put the hospital in clear violation of HIPAA data retention and availability requirements. To restore the server, the IT manager contracted with a local third-party data recovery service provider. With no documented policy or procedure for assessing the capabilities and security compliance of such service providers, the IT support manager selected the company based on their 48-hour turnaround time, and shipped them the damaged hard drives without vetting their data security protocols.

The data recovery was a complete success. Within two days, the recovered data was returned to the IT support manager who uploaded the full database of patient records onto the hospital’s new server and the tape backup system was fully functional again. The IT manager made a note in his files to use the local data recovery service provider again, thinking all had gone quite well.

But all was not well. Several months after the recovery, the hospital discovered that a breach of PHI had occurred during the recovery process. While creating an image of all the data on the drives, the data recovery engineer discovered the database of PHI records, including financial and health care account information. He made a second copy of the database for himself, found the records of a female patient with a description closely matching that of his ailing wife, and altered them to fit his wife’s description perfectly, removing references to the female’s blood type and life-threatening allergy to insulin. His wife used the fraudulent identity to receive surgical treatments for cancerous tumors in her lungs. The engineer used the credit card data found in other records to pay for the surgery, pharmaceuticals, and rehabilitation.

Several of the hospital’s patients began reporting unauthorized purchases on their credit cards. The cause of the security breach was not discovered until the woman whose record was altered received emergency surgery after a car crash. Unconscious when she arrived at the hospital, she died from anaphylactic shock during a simple surgical procedure – an allergic reaction to the insulin she was administered during the operation.
The husband was convinced that his wife’s allergy to insulin was well documented in her health record. After investigating the woman’s health records more closely, it was discovered that her PHI recently had been altered and the changes were traced back to the NYC hospital’s database. The hospital’s forensic team was called in, and the breach was traced to the third-party data recovery service provider and their unscrupulous data recovery engineer, who, it was then revealed, had not been subjected to a background check upon hiring. The data recovery engineer had a criminal history of identity theft.

Reports of the breach, the altered medical records, and the woman’s death were picked up by the media. The hospital posted a public notice of the PHI breach and notification letters were sent to all impacted patients outlining the details of the breach, the PHI disclosed, and who had handled their data. Two years of credit monitoring and fraud resolution services, along with credit and identity theft restoration if needed, were offered by the hospital to all affected individuals. However, the larger threat to the patients was the misuse of their PHI which had gone unmonitored. The hospital’s brand name and image were damaged severely.

An internal study was conducted at the hospital and new protocols were adopted to mitigate the risk of using third-party data recovery vendors. The hospital’s risk management process was updated and the hospital’s chief information security officer (CISO) and the IT manager were fired.

Repercussions of This Scenario

Reputational Repercussions

- Tainted the hospital’s brand and reputation, resulting in a loss of current patients and associated revenue due to the availability and acceptability of other hospitals in the New York City metropolitan area
- Loss of expected level of new patients due to reputational loss
- Loss of one surgeon, who went to work for another hospital due to reputational loss

Financial Repercussions

- Cost of corrective action plan including:
  - Cost of developing, documenting, implementing, and training on new processes and procedures related to contracting with third-party service providers
  - Cost of reconstructing altered records to ensure accuracy for affected individuals
  - Cost of incremental staff for auditing policies and procedures
  - Cost of new hard drives
- Cost of providing ID theft monitoring, fraud resolution services, and credit and ID theft restoration services to affected individuals for two years
- Cost of communications to affected individuals, HHS, and state agencies, including legal review, data management, and postage
- Cost of public relations campaign including content development, legal review, and advertising
- Cost of replacing data back-up services vendor

The financial implications of reportable PHI breaches extend beyond the federal and state fines and penalties to include a myriad of cash and non-cash costs.
Legal/Compliance Repercussions
- HHS Office for Civil Rights (OCR) fines
- State fines
- Loss of payment card industry attestation and cost of re-establishing accreditation
- Lawsuit related to stolen credit cards
- Insurance deductible
- Cost of re-instatement of PCI accreditation

Operational Repercussions
- Cost of new CISO and new IT manager, including recruiting, relocation, and higher salary
- Cost of additional IT security workforce member to audit policies and procedures and deliver training

Clinical Repercussions
- Cost of 14 cases of fraudulent claims processed

The total cost to the organization as a result of this hypothetical breach was over $25 million. (See the details of the costing of this scenario in Chapter 8: Calculating the Cost of a PHI Breach Using PHlve.)

Preventive Measures Related to This Scenario

Policy
- Vetting guidelines that include: third-party verification of the service provider’s data security protocols; proof of compliance with HIPAA/HITECH data privacy/protection guidelines; certification of a secure network; background checks on all employees who handle drives and data during the recovery process; training of recovery engineers to safely manage encryption keys; non-disclosure agreements; and chain-of-custody protocols
- All business associates evaluated by the covered entity’s vendor risk assessment program and include a full security program review
- Mandatory update of security reviews of business associates at least annually

Procedures
- Defined, documented, and repeatable business associate risk management processes
- At least an annual review of business associate security practices
- Strong enforcement practices for failing to adhere to the organization’s policies

For more information, read Appendix D – PHI Threat Scenarios.
At the 2011 annual meeting of the Office of the National Coordinator for Health IT, Leon Rodriguez, the recently appointed director of HHS’s OCR, provided this advice to health care organizations to improve HIPAA compliance and the security of PHI:

- Check that risk assessments are up to date;
- Make sure senior managers are supportive of risk mitigation strategies;
- Review existing compliance programs as well as staff training;
- Ensure vigilant implementation of privacy and security policies and procedures, as well as tough sanctions for violating them;
- Conduct frequent internal compliance audits; and
- Develop a plan for prompt response to breach incidents.77

Director Rodriguez’s statements underscore the need for an enterprise-wide risk management approach. Too often, information security is viewed solely as an IT (information technology) problem. However, such a view is too narrow and masks the larger organizational responsibility.

Information security vulnerabilities hold for the entire enterprise, and lack of recognition of this can result in enterprise under investment in PHI security. Businesses can substantially reduce the negative consequences of a successful cyber incident through risk management across the entire organization.


Together, these publications provide a detailed framework that reviews cybersecurity on an enterprise-wide basis, analyzing cyber issues from a strategic, cross-departmental, and economic perspective. Such a framework allows for better analysis of all aspects of the issue so that it can be better understood, managed, and invested in by CFOs and other senior executives.
While a compliance program developed by such a cross-departmental team will be unique to each organization based on the differing business and security needs, there are three aspects of any compliance program that will help to mitigate the risk of a data breach:

### Policy

Privacy policies contain the overarching principles embraced by the executive members of an organization that establish both the culture as it relates to the importance of safeguarding PHI and their expectations of employees, subcontractors, providers, and business associates. Visible executive support can be formalized through the establishment of a privacy office and active participation by the executive team on a privacy steering committee. Committee membership typically can include the general counsel, compliance officer, privacy officer, security officer, chief medical officer, chief information officer, chief financial officer, and human resources.

A common framework for information security management – such as the ISO/IEC 27001 and 27002 standards and NIST Special publication 800-30 – provides a model for business controls that embody these policies and which can be applied to:
- protection of PHI;
- detection of, and incident response to, a breach; and
- recovery of PHI.

Also notable are ISO 27799 and the HITRUST Common Security Framework, which apply this framework specifically to the health care sector.

### Procedures

Procedures must be developed, documented, and implemented to ensure the effectiveness of the key controls in the policies. Training in an organization’s policies and procedures is imperative to minimize the possibility of one of the most common security breaches: unintentional errors and lack of awareness, typically at the hands of a “non-malicious” insider. Without a strong enforcement program and sanctions for non-compliance, the documentation and implementation of procedures will be ineffective.

It is critical that the executive team actively and visibly supports the policies, and that adherence to the procedures is expected. Investments made in the development, communication, and training of the security program in combination with effective enforcement and sanctions will strengthen the compliance program and provide for the greatest protection of PHI.

Procedures must be augmented by security technologies and address their effectiveness. Investments in security technologies that are either not implemented or ignored by the staff are worthless. Examples include:
- Virus protection turned off by an employee which leaves the system vulnerable to attacks;
- Installed encryption technology without a procedure to encrypt the data; and
- Access controls that are not updated upon job change or termination.
Technology

Examples of the more common information security technical safeguards required in the HIPAA Final Security Rule 164.312 include:

- **Access Control**: Protect ePHI from unauthorized disclosure
  - Allow system access only to authorized persons or applications
  - For a web environment, implement a web access management solution
  - Consider role-based access control
  - Assign unique user identification
  - Ensure the use, monitoring, and audit recording of emergency credentials
  - Establish automatic logoff and re-authentication after a period of inactivity
  - Limit access to encrypted applications to those who can decrypt the data

- **Integrity of Audit Controls**: Protect information from alteration or destruction
  - Implement mechanism to authenticate ePHI
  - Implement methods to corroborate that information has not been altered or destroyed

- **Transmission Security**: Protect ePHI that is being transmitted over a network
  - Consider encryption for best protection and safe harbor
  - Ensure strong encryption up to 2048 bits (asymmetric) and 128 bits (symmetric)
  - Verify data integrity with digital signatures or SSL certificates

In Figure 4 the relationship between policy, procedure, and technology is illustrated for each of the eleven major elements that threaten the security of PHI. Note that policy plays an important role in all threats. Most elements have more than one component and the venn diagram illustrates the interaction between the components.
In order to secure PHI, an organization’s IT department must have documented and implemented procedures and technology in place. While the importance of training cannot be overstated, consider the following list when assessing the current status of security in an organization:

- Risk management (risk identification, threat analysis, etc.)
- Asset management (physical and information)
- Identity management (user IDs, passwords, etc.)
- Physical security (premises protection, visitors, etc.)
- Vulnerability management (secure configuration, patches, etc.)
- Operations management (logs, laptops, desktops, change management, network, mobile devices, removable media, etc.)
- Information protection (encryption, key management, etc.)
- Applications development (code review, testing)
- Threat management (intrusion detection, incident response, etc.)
- Security control testing (penetrations testing, audits, etc.)
- Business continuity (impact analysis, backups, disaster recovery, pandemic planning)
CHAPTER SIX

Survey Findings on Current Practices and Attitudes

In today’s health care environment, information technology has the potential to lower health care spending and to improve the efficiency, quality, and safety of medical care delivery.\(^82\)

Using electronic health records will reduce paperwork and administrative burdens, cut costs, reduce medical errors, and, most importantly, improve the quality of medical care.\(^83\) However, the risk of data breaches increases with the widespread adoption of EHRs and access to digital health information.\(^84\)

Privacy and security controls developed in the era of paper PHI are now outdated, and organizations that are connected in the expanding health care ecosystem need to work together to ensure the protection of shared data.\(^85\)

So with threats, vulnerabilities, and potential safeguards identified, and security and privacy requirements for protecting PHI mandated, how are organizations responding with their compliance programs?\(^86\)

Although almost 60% of respondents in the November 2011 Healthcare Information and Management Systems Society (HIMSS) Security Survey indicated that their IT budget dedicated to information security had increased in the past year, 53% admitted that the total allocated to information security was 3% or less of their operational budgets.\(^86\)

And according to a January 2012 survey of compliance professionals, only 27% of the over 970 participants felt that they have enough resources for their compliance programs. Complicating the situation, those same respondents indicated that their greatest cause of stress was “keeping up with new laws and regulations.”\(^87\)

To provide an understanding of industry reaction to federal and state laws, current levels of compliance, and barriers to strengthening compliance programs, in addition to the frequency and ramifications of PHI breaches, a survey on PHI was circulated to more than two hundred PHI project participants and to other subject matter experts involved in the protection of PHI. The findings from responses of over 100 qualified participants revealed somewhat conflicting insights as to the effectiveness and management support of current privacy programs.\(^88\)

According to a January 2012 survey of compliance professionals, only 27% felt that they have enough resources for their compliance programs.
75% “agreed” or “strongly agreed” with the statement “We have effective policies to protect PHI,” and
76% “agreed” or “strongly agreed” with the statement “We take effective steps to comply”; 
But almost 40% could not agree with the statement that “Management views privacy and security as a priority,” and
54% could not agree with the statement “We possess sufficient resources to ensure requirements are currently being met.”

In the same survey, when asked about the complexity of the laws and the ease of compliance, only 12% felt that they were “easy to understand” and only 14% thought the laws were “not difficult at all” to comply with. Three respondents made the following comments about the laws and regulations:

- “There is so much overlap between laws that analysis is time consuming and difficult.”
- “We do not have the employee resources or the funds to deal with additional federal regulations.”
- “The laws have been ever changing which makes it difficult to keep pace with policies/procedures and training of employees. The process for passage often is annoying because sometimes facilities are expected to comply with the law before it is final.”

How would you characterize the complexity of these laws?

- Easy to understand: 12%
- Complex/difficult to understand: 52%
- Overly complex/vague or confusing: 36%

How easy is it for your organization to comply with these laws?

- Not difficult at all - we have all the resources required to maintain compliance within our organization: 14%
- Somewhat difficult - the current laws place some strain on our organization to maintain compliance: 27%
- Difficult - the current laws place undue stress on our organization to maintain compliance: 59%
When asked to identify the most significant impediments their organization faces to achieving a strong privacy and data security posture with respect to how PHI is collected, used, and retained (multiple answers possible), 59% cited “lack of funding” and 40% indicated “insufficient time.” Almost a third (32%) answered “lack of senior executive support,” and 28% listed “lack of accountability and leadership.”

Although some of the responses indicated that senior management was aware of the great need for security, respondents also indicated that they experienced a lack of senior executive support, and the absence of accountability and leadership in implementing compliance.

One participant stated, “Health care information security is behind the times. Senior leaders need to understand that legacy protection mechanisms like firewalls are no longer adequate.”

**PHI Security Threats**

In response to questions regarding the most likely current threats affecting their organization’s ability to secure PHI, a combined 85% stated that the accidental or inadvertent exposure from an insider was the “most likely” or a “very likely” threat. 56% believed that it is “very likely” or “likely” that the organization’s current threat comes from malicious insiders.

In addition, malware infestation proved to be a great concern for the organizations participating, with 76% seeing this as a “very likely” or “likely” threat. A combined 61% of respondents felt that their organization is “very likely” or “likely” to fall prey to social engineering attacks. More than 50% of respondents believed that some type of security threat was “likely” affecting their organization in an adverse manner now.

A follow-up question asked respondents to indicate whether they believe these threats will worsen within the next three years; 43% thought that state-sponsored attacks would pose a future threat and 55% indicated that it would be “very likely” or “likely” that future attacks may be perpetrated by malicious insiders. A combined 70% of respondents were concerned that security will be compromised by accidental or inadvertent exposure from an insider.
PHI Breaches and the Financial Impact

When asked whether their organization had experienced a data breach in the last twelve months, only 46% responded definitively that their organization had not suffered a data breach.

In response to questions regarding the financial losses suffered by their organizations due to breaches, only 22% of respondents provided an estimate. Those that provided an estimate stated that their costs were for credit or identity theft monitoring, and for forensic and legal fees. A few respondents mentioned losses due to reputational harm, including loss of goodwill and of business. Another mentioned increased insurance cost. The range of total costs by a handful of respondents who provided estimates was between $8,000 and $300,000.

The survey responses revealed that the majority of participants want to comply and secure PHI, but they believe that budgetary constraints and the lack of executive commitment, leadership, and accountability, as well as the evolving nature of threats and the technologies available to protect PHI, combine to make real protection of health information very challenging.

The full results of the survey are available in Appendix E – Complete Results of Survey: Current Practices and Attitudes.
How much should an organization be willing to invest to reduce its risk exposure while gaining a business advantage? An organization that has not suffered a data breach in the last two years is in the minority. The threats to the security of PHI are real, and the incentives for stealing it are financially rewarding.

In addition to the legal and ethical obligations to protect PHI, there is another, very real and equally important reason for protecting it. It is called “goodwill” – the intangible advantages that a company has in its market, including strategic locations, business connections, and, relevant to this matter, an excellent reputation.

Statements prepared under generally accepted accounting principles (GAAP) do not record these “assets,” but an organization’s reputation for PHI protection is, without a doubt, a market advantage and key to the generation of revenue, the retention of customers, and the productivity of the workforce.

Respondents to the previously cited Ponemon survey believe data breaches suffered by their organizations had resulted in time and productivity loss (81%), in diminished brand or reputation (78%), and in loss of patient goodwill (75%).

So, how much should an organization invest to maintain, if not increase, the value of their goodwill?

This chapter describes PHIve – PHI Value Estimator, pronounced five – a 5-step method for PHI protectors to calculate the potential (or actual) cost of a data breach to their organization.

With this ammunition in hand, PHI protectors can determine and recommend the appropriate investments necessary to mitigate the risk of a data breach, thereby reducing potential financial exposure while strengthening their reputation as a protector of the PHI entrusted to their care.
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Conduct a risk assessment: assess the risks, vulnerabilities, and applicable safeguards for each “PHI home.”</td>
</tr>
<tr>
<td>2</td>
<td>Determine a “security readiness score” for each “PHI home” by determining the likelihood of a data breach based on the “security readiness score” scale.</td>
</tr>
<tr>
<td>3</td>
<td>For each “PHI home” that has an unacceptable “security readiness score,” examine the relevance (i.e., likelihood or applicability) of a particular cost category, and apply a “relevance factor” from the relevance factor hierarchy.</td>
</tr>
<tr>
<td>4</td>
<td>Determine the impact: relevance \times consequence = impact.</td>
</tr>
<tr>
<td></td>
<td>- Relevance – determine the “relevance factor” associated with the cost category for your organization</td>
</tr>
<tr>
<td></td>
<td>- Consequence – calculate the potential cost of the cost category based on considerations for your organization</td>
</tr>
<tr>
<td></td>
<td>- Impact – multiply the “relevance factor” the “consequence” to determine the “adjusted cost”</td>
</tr>
<tr>
<td>5</td>
<td>Add up all adjusted costs to determine the total adjusted cost of a data breach to the organization.</td>
</tr>
</tbody>
</table>
Step 1: Conduct a Risk Assessment – Assess the Risks, Vulnerabilities, and Applicable Safeguards for Each “PHI Home”

A “PHI home” is any organizational function or space (administrative, physical, or technical) and/or any application, network, database, or system (electronic) that creates, maintains, stores, transmits, or disposes of ePHI or PHI.

Step 1 involves making a list of every “PHI home” in the organization and in the organizations of any business associates. Assess the potential risk events, vulnerabilities, and applicable safeguards for each organizational function (see examples in Table 4: Determining the Likelihood of Administrative, Physical, and Technical Data Breaches) and for each system/application/database (see examples in Table 5: Determining the Likelihood of Electronic Security Data Breaches).

<table>
<thead>
<tr>
<th>Potential Risk Event</th>
<th>Functional Areas or Responsibilities to Be Considered</th>
<th>Vulnerabilities to Be Considered</th>
<th>Safeguards/Controls to Be Rated</th>
</tr>
</thead>
</table>
| - Physical penetration  
- Physical destruction  
- Sabotage  
- Theft  
- Unauthorized deletion  
- Vandalism  
- Employee error  
- Information disclosure (e.g., shoulder surfing, elevator chat, wrong recipient)  
- Improper training of staff  
- Unavailability of data  
- Fraud | - Reception  
- Clinical treatment areas  
- Data record storage  
- IT support  
- Data disposal  
- Accounting  
- Billing department  
- Audit department  
- Process excellence  
- Accreditation  
- Quality outcomes  
- Human resources  
- Operations reporting  
- Facilities | - Physical theft  
- Intentional or unintentional fax to unauthorized user  
- Intentional or unintentional email to unauthorized user  
- Unsecured email  
- Improper disposal of written documents  
- Unauthorized creation or modification of written documents  
- Unauthorized use of written documents  
- Unauthorized sharing of written documents  
- Mistaken identity  
- Untrained or improperly trained workforce member  
- Failure to establish or update clearance level of workforce member | - New hire background checks  
- Assigned security responsibility  
- Documented and enforced policies and procedures  
- Workforce access authorization clearance processes  
- Regular workforce training  
- Sanctions for non-compliance with policies and procedures  
- Log-in and password management  
- Incident reporting  
- Secure facility access  
- Workstation security and privacy  
- Business associates’ contracts and audits  
- Regular monitoring and/or auditing of procedures |
<table>
<thead>
<tr>
<th>Potential Risk Event</th>
<th>Applications to Be Considered</th>
<th>Vulnerabilities to Be Considered</th>
<th>Safeguards/Controls to Be Rated</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Computer-based attack</td>
<td>- Admit, discharge, and transfer (ADT)</td>
<td>- Lack of encryption/decryption capabilities</td>
<td>- Authentication of authorized users</td>
</tr>
<tr>
<td>- Electronic penetration</td>
<td>- Medication administration record system (MARS)</td>
<td>- Lack of reliable data back-up and recovery</td>
<td>- Strong authentication construction</td>
</tr>
<tr>
<td>- Destruction of files</td>
<td>- Order entry (CPOE) systems or applications</td>
<td>- Multiple system access</td>
<td>- Documented processes and training</td>
</tr>
<tr>
<td>- Destruction of systems</td>
<td>- Imaging (PACS) systems or applications</td>
<td>- LAN, WAN, or external system pathways</td>
<td>- Reviewed and approved clearance for authorized users</td>
</tr>
<tr>
<td>- Sabotage</td>
<td>- Accounting systems or applications</td>
<td>- Network pathways</td>
<td>- Audit controls for identifying unauthorized users</td>
</tr>
<tr>
<td>- Theft of ePHI data</td>
<td>- Billing and receivables systems or applications</td>
<td>- No protection against data interception</td>
<td>- Audit controls for identifying unauthorized activity</td>
</tr>
<tr>
<td>- Unauthorized creation of ePHI</td>
<td>- Electronic record systems or applications</td>
<td>- No protection against hacking</td>
<td>- Encryption and decryption capabilities</td>
</tr>
<tr>
<td>- Unauthorized deletion of ePHI</td>
<td>- Dictation and transcription systems or applications</td>
<td>- No protection against port scanning and sniffing</td>
<td>- Data integrity controls</td>
</tr>
<tr>
<td>- Unauthorized modification of ePHI</td>
<td>- Systems or applications used for utilization reviews</td>
<td>- No protection against social engineering</td>
<td>- Transmission security</td>
</tr>
<tr>
<td>- Vandalism</td>
<td>- Systems or applications used for accreditation</td>
<td>- Flaws in technology and software or protocol designs</td>
<td>- Limited to a single system</td>
</tr>
<tr>
<td></td>
<td>- Systems or applications used for oversight/root cause analysis/governance purposes</td>
<td>- No protocols for peer-to-peer file sharing</td>
<td>- LAN, WAN, or external system is not protected</td>
</tr>
<tr>
<td></td>
<td>- Systems or applications used for auditing, credentialing, litigation</td>
<td>- Missing security agents</td>
<td>- No network pathway or unprotected pathway</td>
</tr>
</tbody>
</table>
Step 2: Determine a “Security Readiness Score” for Each “PHI Home” by Determining the Likelihood of a Data Breach Based on the “Security Readiness Score” Scale

Following a full and robust discussion with a cross-functional team of each risk event, vulnerability, and applicable safeguards – strongly recommended to ensure organizational agreement and a unified position when presenting recommendations – assign a “security readiness score” based on the likelihood of a data breach for each PHI home. The previously cited Internet Security Alliance (ISA) and American National Standards Institute (ANSI) joint publications provide a framework for this type of cross-functional team discussion.

While it is certainly up to the organization to determine its risk appetite, one might view a “security readiness score” of 1 or 2 to be acceptable and a score of 4 or 5 to be unacceptable.

<table>
<thead>
<tr>
<th>Score</th>
<th>The Likelihood of a Data Breach</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Virtually impossible</td>
</tr>
<tr>
<td>2</td>
<td>Rare</td>
</tr>
<tr>
<td>3</td>
<td>Possible but not likely</td>
</tr>
<tr>
<td>4</td>
<td>Possible and likely</td>
</tr>
<tr>
<td>5</td>
<td>Possible and highly likely</td>
</tr>
</tbody>
</table>

Step 3: For Each “PHI home” That Has an Unacceptable “Security Readiness Score,” Examine the Relevance (i.e., Likelihood or Applicability) of a Particular Cost Category, and Apply a “Relevance Factor” from the Relevance Factor Hierarchy

Fines and penalties assessed by the federal and state governments are not the only costs that are included in this calculation. A study found that the organizational costs of data breaches from 2005 to 2010 have exceeded $150 billion, excluding the actual losses sustained by the victims of these breaches. Add to this the costs of the resulting business distraction and the declining value of goodwill and the implications are substantial.

Potential data breach repercussions are broken down into five cost categories: (1) reputational, (2) financial, (3) legal/regulatory, (4) operational, and (5) clinical, which have been further broken down into cost impact categories on the following pages.

Relevance

There will be cost categories that may not be relevant to one entity but are extremely relevant to another. For example, when considering the possible repercussions of reputational damage, the work of the organization is critical to the relevancy and level of impact for those specific cost categories. A lab imaging company may not suffer as severe a reputational impact as a single-physician practice. The financial impact of a data breach suffered by a fulfillment company may not be as severe as that suffered by a hospital.

Hard versus Soft Costs

Some cost categories will be easier to calculate or estimate than others. The more challenging categories will take some time for the team to assess and quantify. Prepare for spirited discussions with the cross-functional team charged with managing this issue.
Business Associates

The HIPAA Privacy Rule protects individuals’ health information by regulating the circumstances under which covered entities may use and disclose PHI, and by requiring covered entities to have safeguards in place to protect the privacy of the information. As part of these protections, covered entities must have contracts or other arrangements in place with business associates that require access to PHI.93

Considerations

Some considerations are provided on the following pages to help stimulate discussions when determining the relevancy and also the potential impact of a particular cost.

When considering the cost categories for each PHI home, assign a relevance factor associated with the likelihood of that cost being incurred if a data breach occurred in that PHI home.

<table>
<thead>
<tr>
<th>Relevance</th>
<th>Relevance Factor</th>
<th>Risk Exposure/Analysis Best Practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardly relevant</td>
<td>0.05</td>
<td>Pre-breach</td>
</tr>
<tr>
<td>A little relevant</td>
<td>0.15</td>
<td></td>
</tr>
<tr>
<td>Somewhat relevant</td>
<td>0.50</td>
<td></td>
</tr>
<tr>
<td>Relevant</td>
<td>0.85</td>
<td></td>
</tr>
<tr>
<td>Highly relevant</td>
<td>0.95</td>
<td></td>
</tr>
<tr>
<td>Breach</td>
<td>1.00</td>
<td>Post-breach</td>
</tr>
</tbody>
</table>
CHAPTER EIGHT  Calculating the Costs of a PHI Breach Using PHIlve

PHI is not just “digital data.” Each file holds the personal history of an individual and, as such, represents a bond of trust between the individual and the organization entrusted with their data. An organization’s ability to maintain that trust is vital to its brand image, reputation, financial success, and longevity.

Therefore, it is not only the hard incremental costs associated with a breach that need to be considered, but also the costs that arise from the impairment of these intangible assets. This should inform your organization’s cost calculations in the following categories: reputational, financial, legal/regulatory, operational, and clinical.

**Step 4: Determine the Impact: Relevance x Consequence = Impact**

This structure largely mimics the common risk assessment formula: “likelihood” x “consequence” = “impact,” where “likelihood” has been changed to “relevance” for use in a “cost category.”

Using the five repercussion categories suggested below, and the following tips regarding the relevance and impact considerations listed in the tables for each, calculate the relevant adjusted cost of a data breach for each PHI home that has an unacceptable security readiness score.
A. Reputational Repercussions

The Financial Impact of Breached Protected Health Information

Table 8: Relevance and Impact Considerations for Reputational Repercussions

<table>
<thead>
<tr>
<th>Relevance Considerations</th>
<th>Impact Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type of business (CE vs. BA)</td>
<td>Size of breach (&gt;500 records?)</td>
</tr>
<tr>
<td>Availability and acceptability of competitive alternatives</td>
<td>Likelihood of harm</td>
</tr>
<tr>
<td></td>
<td>- Type of data</td>
</tr>
<tr>
<td></td>
<td>- Age of affected individuals</td>
</tr>
<tr>
<td></td>
<td>- Income of affected individuals</td>
</tr>
</tbody>
</table>

* "Loss of patients” refers to the individuals who are seeking care (would not typically apply to a BA).

** "Loss of customers” refers to the payer of the services (e.g., for a CE, a health plan may be a customer of a hospital; for a BA, the customer might be a CE. The BA may have more than one CE customer; a subcontractor may have multiple BA customers).

*** Patient churn is the potential result of diminished brand or reputation in combination with the loss of patient goodwill, according to the previously referenced 2011 Ponemon study. The average lifetime value of one lost patient (customer) increased over 5% in the past year.94

The Effect of Viral Communications

Consider the story of a lead singer of a Canadian band who posted a music video on YouTube after his guitar was severely damaged by airport baggage handlers. Within three days, it had been viewed close to three-quarters of a million times.95

Demographics Matter

In a September 2011 study measuring health privacy sensitivity among certain demographics, consumers rated their sensitivity to 14 health data elements on a 1 to 10 scale. Those in the “46 to 65” age group ranked the highest in privacy sensitivity over their younger and older counterparts; likewise those with the highest income.96

Suggested Formulas

- Loss of patients = average revenue per patient x estimated # who would switch to a competitor x a viral factor
- Loss of current customers = average revenue or margin per customer (as appropriate) x # of customers that might switch to a competitor
- Loss of new customers = projected # of new customers discounted for an estimated # who might switch to a competitor x average revenue or margin per customer
- Loss of strategic partners = projected margin per partner x estimated # that would switch to a competitor + cost of identifying and transitioning to new partners
- Loss of staff = average cost of recruiting and training new staff x estimated # of new staff needed as a result of staff losses + (where applicable) average margin not being generated during transition

**B. Financial Repercussions**
Table 9: Relevance and Impact Considerations for Financial Repercussions

<table>
<thead>
<tr>
<th>Relevance Considerations</th>
<th>Impact Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size of breach</td>
<td>Size of breach (&gt;500 records?)</td>
</tr>
<tr>
<td>Complexity of breach</td>
<td>Type of breach (malicious vs. unintentional)</td>
</tr>
<tr>
<td>Strength of safeguards</td>
<td>Likelihood of harm</td>
</tr>
<tr>
<td>Type of data</td>
<td>– Type of data</td>
</tr>
<tr>
<td>Breached party (CE or BA)</td>
<td>– Age of affected individuals</td>
</tr>
<tr>
<td>Type of company (public vs. private)</td>
<td>– Income of affected individuals</td>
</tr>
</tbody>
</table>

Some considerations to help with this costing:

- **Discovery, Notification, and Response Costs**: The costs following a breach have been estimated by Forrester Research to average about $50 per record.97

- **ID Theft Monitoring**: 29% of the respondents in the 2011 Ponemon survey whose organizations had suffered a data breach reported that their data breaches led to cases of identity theft, a 26% increase from the prior year.98
  - When the U.S. Department of Veterans Affairs discovers a loss, theft, or exposure, it routinely offers identity theft protection at an average cost per covered individual of $29.95 a year.99
  - Industry experts estimate that approximately 20% of affected individuals will actually register for ID theft monitoring services.

- **Size of the Data Breach**: Although a company is required to notify HHS of any and all data breaches on an annual basis, breaches involving the records of 500 or more individuals involve significantly more effort, resources, and cost. Notifications to the following are required within specified timeframes:
  - affected individuals,
  - the media,
  - the secretary of HHS, and
  - the attorneys general in the affected states.100

- **Investor Relations Campaign**: Following the recent announcement of a data breach, Sony’s stock dropped 2.3% at the close of trading in Tokyo, which some analysts suggest was the result of a legal and political backlash over Sony’s delay in notifying affected individuals. The long-term effect of the data breach on the stock price will not be known for a while.101

- **Insurance**: At one financial insurer, health care represents about 25% of the data breach insurance business written, but 60% of all claims.102

- **Business Distraction**: Although difficult to calculate, the distraction caused by a breach has a real cost in lost productivity. A Forrester report determined that the cost per breached financial record averages about $30 per record for time diverted from other tasks to deal with bad press and legal responsibilities.103
C. Legal/Regulatory Repercussions

- **Cost of a Corrective Action Plan (CAP):** Whether a result of an audit on behalf of HHS, or an internal risk assessment, corrective action plans can be expensive. For a data breach reported by the regents of the University of California, the resolutions with HHS\(^{104}\) called for a 3-year CAP that included:
  - a complete review, revision, and implementation of policies and procedures;
  - training and monitoring of the workforce;
  - documentation and implementation of sanctions for non-compliance;
  - establishment of a monitor position and monthly reporting requirements on CAP progress;
  - implementation of annual reports on status; and
  - a resolution fee of $865,000.\(^{105}\)

- **Class Action Lawsuits:** In late 2011, lawyers began closing in on a fixed price of $1,000 per affected individual:
  - Class action lawsuits have been filed against the State of Texas for the posting of unencrypted data on possibly 3.5 million state employees, including one that seeks a $1,000 penalty for each individual affected.\(^{106}\)
  - In September 2011, Stanford Hospital & Clinic was hit with a $20 million lawsuit for exposing the PHI of some 20,000 patients ($1,000 per patient).\(^{107}\)
  - A class action lawsuit was filed against the U.S. Department of Defense on October 10, 2011, seeking $1,000 in damages for each of the 4.9 million TRICARE beneficiaries whose records were on a computer tape that was stolen from the car of a government contractor.\(^{108}\)

While recent cases have used the $1,000 per patient metric, the matter is by no means settled. The ultimate cost to the victim and those liable to the victim will continue to be a moving target, since once ePHI is breached, it is nearly impossible to prevent future misuses of the information and potential harm to the victim.
Table 10: Relevance and Impact Considerations for Legal/Regulatory Repercussions

<table>
<thead>
<tr>
<th>Relevance Considerations</th>
<th>Impact Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type of business (public vs. private)</td>
<td>Size of breach (&gt;500 records?)</td>
</tr>
<tr>
<td>Size of breach</td>
<td>Type of breach (malicious vs. unintentional)</td>
</tr>
<tr>
<td>Strength of compliance program and culture</td>
<td>Likelihood of harm</td>
</tr>
<tr>
<td>Number of previous breaches</td>
<td>- Type of data</td>
</tr>
<tr>
<td>Type of data</td>
<td>- Age of affected individuals</td>
</tr>
<tr>
<td>Breached party (CE or BA)</td>
<td>- Income of affected individuals</td>
</tr>
<tr>
<td></td>
<td>- Resident state of affected individuals</td>
</tr>
</tbody>
</table>

- **Location of Affected Individuals**: Currently 46 states have data breach notification laws and the state attorneys general are enforcing them to protect their residents and gain significant settlements. Texas expanded the notification requirements to cover affected non-residents and is imposing further notification requirements for a breach of health information. Although Health Net fully cooperated, provided two years of credit monitoring services, and improved data and equipment security, the Connecticut Insurance Department fined the health insurer $375,000 for the lack of timely notification following a large breach of personal health information in late 2009.

- **State Contract and Tort Law**: In addition to professional enforcement by licensing boards, state tort law and contractual theories may be available to provide redress for individuals whose health information may not have been collected, used, processed, or disclosed appropriately. While the types of actions that may apply are far too numerous to digest in detail, state tort and/or contract or quasi-contract theories for unauthorized disclosure of health information may include the following: (i) negligence; (ii) intentional and/or negligent infliction of emotional distress; (iii) breach of fiduciary duty; (iv) professional malpractice; (v) unjust enrichment; (vi) invasion of privacy; (vii) intrusion upon seclusion; (viii) false light in the public eye; (ix) violation of rights of publicity; (x) defamation; (xi) breach of confidence; (xii) breach of contract implied and/or express; (xiii) harassment; (xiv) prima facie tort; and, (xv) other theories adopting private causes of action from state statute or constitutional law (such as patient Bill of Rights-type theories). These laws apply broadly, since traditional and non-traditional tort theories may apply. Outside of any alleged mental anguish–type damages, if one does not suffer actual monetary damages, the reach of state tort law to provide redress is somewhat of an open issue. However, there are new damages theories that are being advanced based upon the value of the information to an individual. When actual out-of-pocket damages are suffered (for example, where one expends time and/or money to repair their health information records after medical identity theft), tort law may provide retribution to the affected individuals.

- **Criminal Penalties**: HIPAA, as amended by the HITECH Act, provides for criminal penalties for knowingly, and in violation of the law, using or causing to be used a unique health identifier, obtaining individually identifiable health information relating to an individual, or disclosing individually identifiable health information to another person. Those penalties range from $50,000 to $250,000 and/or one to ten years in prison.

- **Civil Penalties**: Civil monetary penalties are also available and were increased to a maximum of $25,000 to $1.5 million depending on whether the person or entity violating the law exercised “reasonable diligence” or the violation was due to “willful neglect.” The secretary of HHS is required to impose a penalty for all violations due to “willful neglect,” defined as “conscious, intentional failure or reckless indifference” to the obligation owed an individual. Failing to comply with requirements of the HIPAA Privacy and Security Rules would likely meet this definition.
Tier A violations: did not realize and would have handled the matter differently -
- $100 fine for each affected individual, and
- $25,000, maximum total imposed for the calendar year.

Tier B violations: due to reasonable cause, but not “willful neglect” -
- $1,000 fine for each affected individual, and
- $100,000, maximum total imposed for the calendar year.

Tier C violations: due to willful neglect, ultimately corrected -
- $10,000 fine each affected individual, and
- $250,000, maximum total imposed for the calendar year.

Tier D violations: willful neglect, uncorrected -
- $50,000 fine for each affected individual, and
- $1,500,000, maximum total imposed for the calendar year.

The HITECH Act authorizes state attorneys general to bring lawsuits against individuals and organizations on behalf of residents for violations of any provisions of the HIPAA and HITECH laws and may recover damages of $100 per violation up to $25,000 in a calendar year, plus attorney’s fees. Some state health privacy laws impose higher monetary penalties on breaching parties, and recently the Indiana attorney general invoked state law, over HIPAA/HITECH, when prosecuting a privacy breach by insurer WellPoint, Inc.

Finally, the HITECH Act requires the secretary of HHS to establish by 2012 a methodology by which any individual harmed by a violation of the HIPAA or HITECH Acts may recover a percentage of any civil monetary penalty or monetary settlement. This provision is likely to increase the number of complaints that cite violations of the privacy and security laws.

D. Operational Repercussions

<table>
<thead>
<tr>
<th>Relevance Considerations</th>
<th>Impact Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sufficiency of current resources</td>
<td>Number of additional resources needed</td>
</tr>
<tr>
<td>Appropriateness of placement of compliance program in organizational structure</td>
<td>Level of disruption of required organizational changes</td>
</tr>
</tbody>
</table>

In addition to any remediation or corrective action plan (CAP) required by OCR, additional operational costs associated with strengthening a compliance program may be necessary or appropriate following a data breach. These costs might include hiring outside consultants to design and/or deliver a more effective training program or the hiring of additional employees with needed skills, knowledge, and experience, to handle technology security requirements. In some cases, a higher-level employee in the organization may be needed to heighten awareness and strengthen the power of the decisions to be made. Organizational changes often disrupt the organization for a period of time, which comes with a loss of productivity.
E. Clinical Repercussions

The rise of medical identity theft has led to increased costs for the health care industry and the victims. Schemes involve the lending and borrowing of a valid ID to access health care services. Over one third (36%) of provider organizations participating in the PwC survey confirmed that they have experienced patients seeking services using somebody else’s name and identification.

Medical identity theft is especially expensive and potentially dangerous for the victim. If medical files have been altered, it can lead to the administration of incorrect care with disastrous results. It can result in the mistaken belief that the victim is ineligible for both life and health insurance. Misdirected and unpaid medical bills can result in damage to credit scores.

The result of these complications is that the average financial damage done to the clinical fraud victim can be as much as $20,000, a cost increasingly being borne by the covered entity as the responsible party for the PHI breach.

In addition, any medical research utilizing inaccurate data from altered medical records to create new evidence-based care could lead to future patients either receiving improper care or having proper care withheld or delayed.

<table>
<thead>
<tr>
<th>Table 12: Relevance and Impact Considerations for Clinical Repercussions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Relevance Considerations</strong></td>
</tr>
<tr>
<td>■ Type of data (prescription vs. medical care)</td>
</tr>
<tr>
<td>■ Intent (malicious vs. unintentional)</td>
</tr>
<tr>
<td>■ Age and income of affected individuals</td>
</tr>
<tr>
<td>■ Number of records breached</td>
</tr>
</tbody>
</table>
Step 5: Add up All Adjusted Costs to Determine the Total Adjusted Cost of a Data Breach to the Organization

A number of studies and surveys have provided an average, or estimate, of the total cost of a data breach, and some have turned that total cost into a cost per record breached. But not every data breach is the same, and not every organization that experiences a data breach will incur the same costs. As the previous pages have pointed out, the relevance and impact considerations can drive a wide range of liabilities.

In order to determine a customized cost of a data breach to your organization, total up all adjusted costs for all PHI homes that have an unacceptable security readiness score to determine a total adjusted cost of a data breach to your organization. Compare that total adjusted cost to the table at right to determine the significance level of a data breach to your organization given its current level of threats, risks events, vulnerabilities, and safeguards.

Armed with this total adjusted cost and the potential total impact of a breach to your organization, in addition to the assessments, security readiness scores, relevance and impact considerations, relevance factors, and adjusted costs, you can determine and recommend a solid rationale for an investment in strengthening your compliance program along with a list of prioritized risk mitigation initiatives.

**How Much Should Be Invested to Strengthen a Privacy and Security Program?**

To determine a recommended level of investment, a quantitative risk assessment method involves the calculation of the annualized loss expectancy (ALE) of a data breach. Multiply the average cost of one incident (also known as single loss expectancy or SLE) by the probability that the incident will occur during one year (also known as the annualized rate of occurrence or ARO).

\[
\text{ALE} = \text{SLE} \times \text{ARO}
\]

The SLE in this case is the total adjusted cost calculated above. The ARO will be a much discussed factor for your team, and will be based on the level of safeguards and controls that your organization has in place, your history of breaches and remediation actions, and those of your business associates and subcontractors.

As a reminder, from the 2011 Ponemon study, 96% of the provider organizations studied reported having had at least one data breach in the past 24 months.  

An example of the costing of a data breach specific to the hypothetical scenario presented in chapter four is provided on the next pages, including relevance and impact considerations, followed by calculations of those costs based on estimates and statistical studies.

Assuming the probability that the organization in the scenario will incur a breach every two years, the ARO = \(\frac{1}{2}\) or 50%, which when multiplied by the SLE of $26,493,617 (total adjusted cost of a breach) results in an ALE of $13,246,809.
If an investment in strengthening the privacy and security program could reduce the probability of a data breach from once every two years to once every five years, the ARO would become $\frac{1}{5}$ (or 20%), which when multiplied by the SLE of $26,493,617$ results in an ALE of $5,298,723$.

The reduction in the ALE from today’s exposure of $13.2$ million to a potential exposure of $5.3$ million supports an investment of $7.9$ million in initiatives that can produce that level of reduction in the probability of a breach. (Note: $7.9$ million is approximately 3.3% of that organization’s annual revenue.)

And, do bear in mind the following: “On average, the breached firms lost 2.1 percent of their market value within two days following the public announcement.”122 The cost of an internally developed corrective action plan is a direct investment in your organization’s reputation as a protector of PHI.
<table>
<thead>
<tr>
<th>COST CATEGORY</th>
<th>COST IMPACT CATEGORY</th>
<th>COST SUB-CATEGORY</th>
<th>RELEVANCE CONSIDERATIONS</th>
<th>IMPACT CONSIDERATIONS</th>
<th>TOTAL COST</th>
</tr>
</thead>
<tbody>
<tr>
<td>REPUTATIONAL</td>
<td>LOSS OF CURRENT</td>
<td>AVAILABLE ALTERNATIVES IN NYC</td>
<td>WOMAN’S WRONGFUL DEATH SEVERELY DAMAGES REPUTATION</td>
<td>$ 8,947,947</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PATIENTS/CUSTOMERS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>LOSS OF NEW BUSINESS</td>
<td>AVAILABLE ALTERNATIVES IN NYC</td>
<td>WOMAN’S WRONGFUL DEATH SEVERELY DAMAGES REPUTATION</td>
<td>$ 1,934,691</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LOSS OF STAFF</td>
<td>AVAILABLE ALTERNATIVES IN NYC</td>
<td>IMPORTANCE OF REPUTATION; AVAILABILITY AND COST OF PROFESSIONAL STAFF</td>
<td>$ 110,000</td>
<td></td>
</tr>
<tr>
<td>REMEDIATION</td>
<td>CORRECTIVE ACTION PLAN</td>
<td>MODIFICATION OF DISASTER RECOVERY AND BUSINESS CONTINUITY POLICIES TO INCLUDE HARD DRIVE FAILURES; ESTABLISH AUDIT AND SECURITY VETTING PROCEDURES FOR DATA RECOVERY VENDORS; RECONSTRUCT ALTERED RECORDS</td>
<td>AVAILABILITY OF RESOURCES TO DOCUMENT, IMPLEMENT AND TRAIN ON NEW PROCEDURES, # OF RECORDS ALTERED, COST OF NEW EQUIPMENT</td>
<td>$ 2,452,780</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WORKFORCE SANCTIONS</td>
<td>FIRED CEO AND IT MANAGER</td>
<td>AVAILABILITY OF REPLACEMENT STAFF, COST OF RECRUITING AND REPLACEMENT SALARIES</td>
<td>$ 81,000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ID THEFT MONITORING</td>
<td># OF RECORDS; TYPE OF INFORMATION</td>
<td># OF YEARS PROVIDED</td>
<td>$ 3,430,129</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LOSS OF PRODUCTIVITY</td>
<td>COMPLEXITY OF BREACH</td>
<td># OF AFFECTED INDIVIDUALS; MAGNITUDE OF CHANGES</td>
<td>$ 48,000</td>
<td></td>
</tr>
<tr>
<td>COMMUNICATION</td>
<td>EFFECTED INDIVIDUALS</td>
<td>SIZE OF BREACH &gt;500 RECORDS</td>
<td>DEATH RESULTING FROM BREACH</td>
<td>$ 1,086,550</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MEDIA</td>
<td>SIZE OF BREACH</td>
<td>DEATH RESULTING FROM BREACH</td>
<td>$ 5,000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HHS/STATE AG</td>
<td>SIZE OF BREACH</td>
<td>USE OF OUTSIDE CONSULTANTS, COST OF ADVERTISING</td>
<td>$ 305,000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PUBLIC RELATIONS</td>
<td>SIZE OF BREACH, REPUTATION IN COMMUNITY</td>
<td>USE OF THIRD-PARTY INDEPENDENT SECURITY AUDITORS</td>
<td>$ 18,000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CHANGE IN VENDORS</td>
<td>LEVEL OF PREVIOUS COMPLIANCE</td>
<td>USE OF THIRD-PARTY INDEPENDENT SECURITY AUDITORS</td>
<td>$ 18,000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(IF BA-RELATED)</td>
<td>INCREASED AUDITS TO ENSURE COMPLIANCE</td>
<td>DEATH AS A RESULT OF TRANSACTIONS</td>
<td>$ 15,000</td>
<td></td>
</tr>
<tr>
<td>LEGAL</td>
<td>OCR</td>
<td>WRONGFUL DEATH; ACCOUNTABILITY: LACK OF VETTING POLICY AND PROCEDURES FOR SERVICE PROVIDER’S DATA SECURITY PROTOCOLS, PROOF OF COMPLIANCE AND SECURITY CERTIFICATION</td>
<td>HOSPITAL COOPERATED, BUT THE NEGLIGENCE ASSOCIATED WITH VETTING 3RD-PARTY VENDOR DETERMINED “WILLFUL NEGLECT”</td>
<td>$ 250,000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>STATE AG</td>
<td>SIZE OF BREACH</td>
<td>UNWANTED DEATH</td>
<td>$ 338,000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LAWSUIT</td>
<td>LEGAL, SETTLEMENT, ADDITIONAL PAYMENTS &amp; INSURANCE DEDUCTIBLE</td>
<td>UNWANTED DEATH</td>
<td>$ 9,739,880</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LOSS OF ACCREDITATION</td>
<td>PCI</td>
<td>FINANCIAL FRAUD</td>
<td>RE-ESTABLISH ACCREDITATION</td>
<td>$ 793,000</td>
</tr>
<tr>
<td>OPERATIONAL</td>
<td>COST OF NEW HIRE</td>
<td>BA-RELATED BREACH, NO ADDITIONAL STAFF NEEDED</td>
<td>ADDED STAFF IN REMEDIATION PLAN</td>
<td>$ -</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FRAUD</td>
<td>TYPE OF DATA: PRESCRIPTION MORE FREQUENT BUT LESS COSTLY VS. FREE MEDICAL CARE: LESS FREQUENT BUT MORE COSTLY</td>
<td>$ 94,640</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

GRAND TOTAL COST OF DATA BREACH $ 26,493,617

TOTAL ANNUAL REVENUE OF CLAIMS PAID $ 241,836,404

% OF DATA BREACH COST TO TOTAL ANNUAL REVENUE 11%

<table>
<thead>
<tr>
<th>IMPACT</th>
<th>Cost/Record</th>
<th>Cost/Affected Individual</th>
<th>Annualized Lost Expenditure*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severe</td>
<td>$ 31.35</td>
<td>$ 7,838.35</td>
<td>$ 5,298,723</td>
</tr>
</tbody>
</table>

*the cost of risk for one year based on the probability that the incident will occur during one year assuming a data breach once every (8 years) 5

Scoring the Total Impact:

- Significant: Less than 2% of Revenue
- Minor: 2% of Revenue
- Moderate: 4% of Revenue
- Major: 6% of Revenue
- Disaster: Greater than 6% of Revenue

Calculation of the Annualized Lost Expenditures:

- Single Lost Expenditure (ALE) = the average cost of one incident $ 26,493,617
- Annualized Rate of Occurrence (ARO) = the probability that the incident will occur during one year 0.20
- Annualized Lost Expenditure (ALE) the cost of risk for one year: ALE = ALE * ARO $ 5,298,723
Selected Calculations of Costs Incurred by the Hospital in the Hypothetical Scenario Provided in Chapter 4 (These calculations are based on the details of this hypothetical example; specific analysis for an organization should reflect the relevance and impact for that organization.)

<table>
<thead>
<tr>
<th>Line #</th>
<th>Description</th>
<th>Our Example</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Annual Hospital Revenue</td>
<td>$241,836,404</td>
<td>This example: from hospital records</td>
</tr>
<tr>
<td>2</td>
<td># of Patients in year</td>
<td>845,000</td>
<td>This example: records breached</td>
</tr>
<tr>
<td>3</td>
<td>% of Unique Patients</td>
<td>37.5%</td>
<td>This example: % of unique patients</td>
</tr>
<tr>
<td>4</td>
<td># of Unique Patients</td>
<td>316,875</td>
<td>line 2 * line 3</td>
</tr>
<tr>
<td>5</td>
<td>Revenue/Unique Patient</td>
<td>$763.19</td>
<td>line 1 / line 4</td>
</tr>
<tr>
<td>6</td>
<td>Patient churn due to reputational harm</td>
<td>3.70%</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Revenue Loss associated with loss of active patients</td>
<td>$8,947,947</td>
<td>line 4 * line 5 * line 6</td>
</tr>
<tr>
<td>8</td>
<td>Loss of New Patients:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Forecast % of new active patients next year</td>
<td>10%</td>
<td>This example: from Finance Budgeting assumptions</td>
</tr>
<tr>
<td>10</td>
<td>Expected # of new patients per year</td>
<td>31,688</td>
<td>line 4 * line 8</td>
</tr>
<tr>
<td>11</td>
<td>Projected new revenue</td>
<td>$24,183,640</td>
<td>line 5 * line 9</td>
</tr>
<tr>
<td>12</td>
<td>% revenue loss due to negative publicity</td>
<td>8%</td>
<td>This example: 20% reduction in forecast new business (financial estimates of viral impact) and availability of competition</td>
</tr>
<tr>
<td>13</td>
<td>Loss of New Patient Revenue</td>
<td>$1,934,691</td>
<td>line 10 * line 11</td>
</tr>
<tr>
<td>14</td>
<td>Loss of Strategic Partners:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Recruiting Cost</td>
<td>$80,000</td>
<td>all health plans stayed with the hospital</td>
</tr>
<tr>
<td>16</td>
<td>Incremental higher salary of new surgeon</td>
<td>$30,000</td>
<td>Replaced one cardiothoracic surgeon who quit and joined competitor</td>
</tr>
<tr>
<td>17</td>
<td>Loss of Staff</td>
<td>$110,000</td>
<td>line 14 + line 15</td>
</tr>
<tr>
<td>18</td>
<td>Total Reputation Repercussions</td>
<td>$10,992,638</td>
<td>line 7 + line 12 + line 13 + line 16</td>
</tr>
<tr>
<td>19</td>
<td>Financial Repercussions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Cost of Remediation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>a Investigation and Forensic Costs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>b Cost of Corrective Action Plan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>Cost of Documenting, Implementing &amp; Training New Procedures</td>
<td></td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>Cost of Reconstructing Records</td>
<td></td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>Total Cost of Rebuilding Records</td>
<td>$2,132,780</td>
<td>line 22 * line 23</td>
</tr>
<tr>
<td>27</td>
<td>Cost of incremental staff for auditing policies and procedures</td>
<td></td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>Cost of new hard drives</td>
<td></td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>Total Cost of Corrective Action Plan</td>
<td>$4,252,780</td>
<td>line 19 + line 24 + line 25 + line 26</td>
</tr>
<tr>
<td>30</td>
<td>c Workforce Sanctions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>Recurring Cost</td>
<td></td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>Incremental Higher Salaries &amp; Benefits</td>
<td></td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>Total Cost of Workforce Sanctions</td>
<td>$81,000</td>
<td>line 28 + line 29</td>
</tr>
<tr>
<td>34</td>
<td>d ID Theft Monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td>35</td>
<td># of records breached</td>
<td>845,000</td>
<td>This example: # of records breached</td>
</tr>
<tr>
<td>36</td>
<td>% of individuals needing Credit Monitoring</td>
<td>0.40%</td>
<td>FBI Fraud Estimate</td>
</tr>
<tr>
<td>37</td>
<td>% of individuals needing Credit Monitoring</td>
<td>3.380</td>
<td>Meeting at the University of Advanced Technologies</td>
</tr>
<tr>
<td>38</td>
<td>Cost of Credit Monitoring/affected individual/year</td>
<td></td>
<td></td>
</tr>
<tr>
<td>39</td>
<td>Cost of Credit Monitoring for affected individuals for two years</td>
<td>$215,982</td>
<td>line 33 * line 34 * 2 years</td>
</tr>
<tr>
<td>40</td>
<td># of individuals eligible for Fraud Watch</td>
<td>841,620</td>
<td>line 23 * line 25</td>
</tr>
<tr>
<td>41</td>
<td>% of individuals who will take advantage of Fraud Watch</td>
<td>19%</td>
<td>from industry experts</td>
</tr>
<tr>
<td>42</td>
<td>Cost of ID Fraud Watch/non-affected individuals/year</td>
<td></td>
<td></td>
</tr>
<tr>
<td>43</td>
<td>Cost of ID Fraud Watch for non-affected individuals for two years</td>
<td>$3,214,147</td>
<td>line 38 * line 39 * 2 years</td>
</tr>
<tr>
<td>44</td>
<td>Total Cost of ID Theft Monitoring for two years</td>
<td>$3,480,329</td>
<td>line 35 + line 40</td>
</tr>
</tbody>
</table>
The Financial Impact of Breached Protected Health Information

<table>
<thead>
<tr>
<th>line #</th>
<th>Our Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td></td>
</tr>
<tr>
<td>Cost of Lost Productivity</td>
<td></td>
</tr>
<tr>
<td># of months between discovery to remediation resolution</td>
<td>42</td>
</tr>
<tr>
<td>% decline in productivity</td>
<td>43</td>
</tr>
<tr>
<td>semi-annual payroll for IT personnel</td>
<td>44</td>
</tr>
<tr>
<td>Total Cost of Lost Productivity</td>
<td>45</td>
</tr>
<tr>
<td>Total Cost of Remediation</td>
<td>46</td>
</tr>
</tbody>
</table>

Cost of Communication

<table>
<thead>
<tr>
<th>line #</th>
<th>Our Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td></td>
</tr>
<tr>
<td>Notification to Affected Individuals</td>
<td></td>
</tr>
<tr>
<td>Affected Individuals</td>
<td>47</td>
</tr>
<tr>
<td>Message Development</td>
<td>48</td>
</tr>
<tr>
<td>Legal Review</td>
<td>49</td>
</tr>
<tr>
<td>Total Notification Cost to Affected Individuals</td>
<td>52</td>
</tr>
<tr>
<td>b</td>
<td></td>
</tr>
<tr>
<td>Notification to Media</td>
<td></td>
</tr>
<tr>
<td>Message Development</td>
<td>53</td>
</tr>
<tr>
<td>Legal Review</td>
<td>54</td>
</tr>
<tr>
<td>Total Notification Costs to Media</td>
<td>56</td>
</tr>
<tr>
<td>c</td>
<td></td>
</tr>
<tr>
<td>Notification to HHS/State Agencies</td>
<td></td>
</tr>
<tr>
<td>Message Development</td>
<td>57</td>
</tr>
<tr>
<td>Legal Review</td>
<td>58</td>
</tr>
<tr>
<td>Total Notification Costs to HHS/State Agencies</td>
<td>60</td>
</tr>
<tr>
<td>d</td>
<td></td>
</tr>
<tr>
<td>Public Relations Campaign</td>
<td></td>
</tr>
<tr>
<td>Campaign Development</td>
<td>61</td>
</tr>
<tr>
<td>Legal Review</td>
<td>62</td>
</tr>
<tr>
<td>Business Distraction of CEO/CFO (interviews)</td>
<td>64</td>
</tr>
<tr>
<td>Total Public Relations Campaign Cost</td>
<td>65</td>
</tr>
<tr>
<td>Total Cost of Communication</td>
<td>66</td>
</tr>
</tbody>
</table>

Cost of Increased Insurance Coverage

<table>
<thead>
<tr>
<th>line #</th>
<th>Our Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td></td>
</tr>
<tr>
<td>Broker Fees</td>
<td>67</td>
</tr>
<tr>
<td>b</td>
<td></td>
</tr>
<tr>
<td>Presentation and Negotiation Time</td>
<td></td>
</tr>
<tr>
<td>c</td>
<td></td>
</tr>
<tr>
<td>Business Distraction of Financial Resources</td>
<td></td>
</tr>
<tr>
<td>d</td>
<td></td>
</tr>
<tr>
<td>Total Cost of Increased Insurance Coverage</td>
<td></td>
</tr>
<tr>
<td>Total Cost of Increased Insurance Coverage</td>
<td>71</td>
</tr>
</tbody>
</table>

Cost of Changing Business Associate [Data Backup]

<table>
<thead>
<tr>
<th>line #</th>
<th>Our Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td></td>
</tr>
<tr>
<td>Cost of Due Diligence on New Data Back-up Vendor</td>
<td></td>
</tr>
<tr>
<td>b</td>
<td></td>
</tr>
<tr>
<td>Cost of Transition Time to New Vendor</td>
<td></td>
</tr>
<tr>
<td>c</td>
<td></td>
</tr>
<tr>
<td>Increased Annual Cost of New Vendor</td>
<td></td>
</tr>
<tr>
<td>Total Cost of Changing Business Associate</td>
<td></td>
</tr>
<tr>
<td>Total Cost of Changing Business Associate</td>
<td>75</td>
</tr>
</tbody>
</table>

Total Financial Repercussions

<table>
<thead>
<tr>
<th>line #</th>
<th>Our Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Financial Repercussions</td>
<td>76</td>
</tr>
</tbody>
</table>

Legal & Regulatory Repercussions

OCR Fines, Penalties and CAP costs

<table>
<thead>
<tr>
<th>line #</th>
<th>Our Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td></td>
</tr>
<tr>
<td>Fines</td>
<td></td>
</tr>
<tr>
<td># of Altered Records</td>
<td>77</td>
</tr>
<tr>
<td>Tier C Violation: &quot;due to willful neglect; ultimately corrected&quot;</td>
<td>78</td>
</tr>
<tr>
<td>b Penalties</td>
<td>79</td>
</tr>
<tr>
<td>c Additional Corrective Action Plan costs</td>
<td></td>
</tr>
<tr>
<td>Monthly and Annual reports on progress</td>
<td>80</td>
</tr>
<tr>
<td>Total OCR Fines, Penalties and CAP costs</td>
<td>81</td>
</tr>
</tbody>
</table>

State Fines and Penalties

<table>
<thead>
<tr>
<th>line #</th>
<th>Our Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td></td>
</tr>
<tr>
<td>Fines</td>
<td></td>
</tr>
<tr>
<td># of Altered Records</td>
<td>82</td>
</tr>
<tr>
<td>NY State AG</td>
<td>83</td>
</tr>
<tr>
<td>b Penalties</td>
<td>84</td>
</tr>
<tr>
<td>Total State Fines &amp; Penalties</td>
<td>85</td>
</tr>
<tr>
<td>Line #</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>86</td>
<td>Legal Costs</td>
</tr>
<tr>
<td>87</td>
<td>Settlement Costs</td>
</tr>
<tr>
<td>88</td>
<td>Additional Payments to Affected Individuals</td>
</tr>
<tr>
<td>89</td>
<td>Insurance Deductible</td>
</tr>
<tr>
<td>90</td>
<td>Credit Card Fraudulent Claims Processed</td>
</tr>
<tr>
<td>91</td>
<td>% of Records Exploited</td>
</tr>
<tr>
<td>92</td>
<td>Impact Card holders</td>
</tr>
<tr>
<td>93</td>
<td>Average Loss per Card</td>
</tr>
<tr>
<td>94</td>
<td>Total Fraudulent Claims Processed</td>
</tr>
<tr>
<td>95</td>
<td>Total Lawsuit Costs</td>
</tr>
<tr>
<td>96</td>
<td>Reinstatement of Accreditation</td>
</tr>
<tr>
<td>97</td>
<td>Total Legal and Regulatory Recurrences</td>
</tr>
<tr>
<td>98</td>
<td>Incremental Cost of New Hires</td>
</tr>
<tr>
<td>99</td>
<td>Cost of Recruiting &amp; Training New Hires</td>
</tr>
<tr>
<td></td>
<td>Cost of Reorganization</td>
</tr>
<tr>
<td>100</td>
<td>Total Operational Recurrences</td>
</tr>
<tr>
<td>101</td>
<td>Fraudulent Claims Processed</td>
</tr>
<tr>
<td>102</td>
<td>% of Medical Fraudulent Claims Processed</td>
</tr>
<tr>
<td>103</td>
<td>Average cost per claim</td>
</tr>
<tr>
<td>104</td>
<td>Total Cost of Fraudulent Medical Claims Processed</td>
</tr>
<tr>
<td>105</td>
<td>Delayed or Inaccurate Diagnosis</td>
</tr>
<tr>
<td>106</td>
<td>Total Clinical Recurrences</td>
</tr>
<tr>
<td>107</td>
<td>Total Impact of Data Breach</td>
</tr>
<tr>
<td>108</td>
<td></td>
</tr>
</tbody>
</table>

Operational Recurrences

Cost of Recruiting & Training New Hires
Cost of Reorganization

Clinical Recurrences

% of Medical Fraudulent Claims Processed
Average cost per claim
Total Cost of Fraudulent Medical Claims Processed
Delayed or Inaccurate Diagnosis

Total Clinical Recurrences
Total Impact of Data Breach
The health care ecosystem is trying to keep in step with today’s technology, reflected in its move to adopt electronic health records.

However, in the course of making this dramatic change to the way health care data is created, stored, and transmitted, the safeguarding of protected health information is not always given top priority.

With the increase in nefarious intent as well as the rewards and opportunities to steal PHI, the likelihood of a data breach for most organizations is very high.

No organization can afford to ignore the potential consequences of a data breach.

Recognize the Risks

To successfully mitigate data breach threats and risks, leaders of organizations in the health care sector must understand the evolving health care ecosystem, and the role that their organization and their subcontractors play in it.

They need to ensure that their organization complies with evolving federal and state health care regulations, and they must understand that non-compliance may result in fines and civil penalties, imposed on both the organization and its leaders.

And they should be aware that, in the future, non-compliance may rise to the level of a criminal offense.

But these are not the only costs and concerns facing organizational leaders. The repercussions of a data breach can be very high and long-lasting – lost business due to reputational harm; penalties, fines, and corrective action plans assessed by HHS and state attorneys general; and the business distraction and impact of increasing class action suits, legal costs, and settlements.
Implement Safeguards and Controls

Organizations entrusted with the protection of PHI need to have a comprehensive understanding of where their PHI is stored, and how it is shared with third parties. All internal and external information flows, as well as threats and vulnerabilities, should be assessed. A sound analysis of the likelihood and impact of a data breach should be undertaken using PHILive, the 5-step method described in this report.

Preventing or detecting a breach requires that effective policies, procedures, and technologies are in place. It is important to gain executive support and develop a good business plan to secure sufficient resources for execution. While it is impossible to eliminate all risks, many can be mitigated in order to reduce significantly the likelihood and impact of a breach, and to ensure that ethical and legal requirements are met. Recommendations for prioritized investments in an enhanced security program, resulting from conducting an organizational risk assessment, can be paid for by the reduced likelihood of a breach.

Those who follow this approach will improve their organization's security posture as well as its bottom line. They also deserve a gracious “thank you” from all the people who trust them to protect their most personal health information.
ENDNOTES


7 Id. at p. 6.


45 C.F.R. § 164.104;HITECH Act, section 13404(a).

45 C.F.R. § 164.520(b)(1)(iv).

The Glossary of this report includes a widely accepted definition of “health information privacy” which has been adopted by the National Committee on Vital and Health Statistics – the organization on which the Secretary of HHS is to rely in implementing HIPAA. See section 1172(f) of HIPAA.


MiddleGate Med proprietary research, May 2011.


85 Ibid.


89 American National Standards Institute (ANSI), The Santa Fe Group / Shared Assessments Program, Internet Security Alliance (ISA), PHI Project Survey.


The Financial Impact of Breached Protected Health Information


45 CFR 164, Subpart A.


Ibid.


HIPAA, section 1177.

HITECH Act, section 13410(d).

HITECH Act, section 13410(c)(2); 45 C.F.R. § 160.401.

HITECH Act, section 13410(e).


HITECH Act, section 13410(c).

Ibid.

Ibid.
According to Dr. Sean Scorvo, MD, ER physician, and CEO of MiddleGate Med, from studies conducted by MiddleGate Med, an emergency room fraud alert service.


Project Leadership

The American National Standards Institute (ANSI – www.ansi.org) is a private non-profit organization whose mission is to enhance U.S. global competitiveness and the American quality of life by promoting, facilitating, and safeguarding the integrity of the voluntary standards and conformity assessment system. The ANSI Identity Theft Prevention and Identity Management Standards Panel (IDSP) is a cross-sector coordinating body that facilitates the timely development, promulgation, and use of voluntary consensus standards and guidelines that will equip and assist the private sector, government, and consumers in minimizing the scope and scale of identity theft and fraud.

The Shared Assessments Program (www.sharedassessments.org) was created by leading financial institutions, the Big Four accounting firms, and key service providers to inject standardization, consistency, speed, efficiency, and cost savings into the service provider assessment process. The Shared Assessments Program is the premiere provider of vendor risk management solutions and tools, which focus on establishing industry best practices, lowering the cost and improving the efficiency of the vendor risk assessment process. Through membership and use of the Shared Assessments tools, Shared Assessments offers outsourcers and their service providers a faster, more efficient, and less costly means of conducting rigorous assessments of controls for security, privacy, and business continuity. Since its inception, the Shared Assessments Program has been managed by The Santa Fe Group, a strategic consulting company.

The Internet Security Alliance (ISA – www.isalliance.org) is a multi-sector trade association established in collaboration with Carnegie Mellon University in 2000. ISA represents an array of organizations concerned with information security from the aviation, banking, communications, defense, education, financial services, insurance, manufacturing, security, and technology sectors. The ISA mission is to combine advanced technology with business economics and public policy to create a sustainable system of world-wide cybersecurity. ISA advocates a modernized social contract between industry and government that would create market-based incentives to motivate enhanced security of cyber systems. ISA provides its members with technical, business, and public policy services to assist them in fulfilling their mission.

Premium Sponsors

Clearwater Compliance (www.clearwatercompliance.com) helps covered entities, business associates, and their subcontractors assess their HIPAA-HITECH compliance programs, identify gaps, and prioritize remediation efforts to ensure the greatest return on capital and resource investments. With the help of proprietary, easy-to-use software, templates, and toolkits, compliance officers can quickly establish a practical corrective action plan tailored specifically to their organization and create a strong competitive positioning as it relates to safeguarding PHI.

DriveSavers Data Recovery (www.drivesaversdatarecovery.com), the worldwide leader in data recovery services, provides fast, reliable, and certified secure data recovery service. DriveSavers is the only company in the data recovery industry to post proof of annual, company-wide SAS 70 Type II Audit Reports and its compliance with the HIPAA security rule. DriveSavers adheres to U.S. government security protocols, the Gramm-Leach-Bliley Act, the Sarbanes-Oxley Act of 2002, the Family Educational Rights and Privacy Act, and the National Institute of Standards and Technology’s SP 800.34 (Rev.1). DriveSavers engineers are certified in all leading encryption and forensics technologies and operate a Certified ISO 5 cleanroom.

Partner Sponsors
“Patients historically trust their doctors to be data stewards of their private health information in paper charts. As healthcare moves from paper to digital in the new age of networked electronic health records, this important publication is convincing and educational about how the broader healthcare system must work hard to earn the same trust that patients have in their doctors to protect their personal and private health information.”

– Dr. Robert Wah, Chief Medical Officer, CSC; Chairman-elect, American Medical Association Board of Trustees

“The PHI study is the front end of a much needed effort to get ahead of those who would penetrate the data systems of our health care providers.”

– John R. Powers, Commissioner and Executive Director, President’s Commission on Critical Infrastructure Protection, 1996-98; Career Senior Executive and FEMA Regional Director, 1993-95

“An indispensable resource for those wrestling with the challenges of PHI security risk.”

– Dr. Michael Kraten, Assistant Professor of Accounting, Providence College; President, Enterprise Management Corporation

“This publication is a must read. It provides not only very useful background information, but also numerous examples of what can happen when appropriate steps are not taken to ensure protected health information integrity. Beyond that, it offers a framework for organizations to assess their security and compliance programs, and it provides a tool for estimating the impact of security breaches on multiple levels.

“No one – not C-level executives, not health care administrators, not Boards of Directors – can afford to ignore its message.”

– Dr. John Fox, President, FFC Computer Services, Inc.

“In this era of emerging awareness of the responsibility and legal requirement to ensure the confidentiality, integrity, and availability of individuals’ protected health information (PHI), as well as the consequences of disregard, business leaders and executives are quickly coming to realize several maxims: first, it’s about business risk management rather than an ‘IT problem;’ second, it requires a programmatic approach; and, third, the C-suite owns this one.

“Smart leaders and managers who care about revenue and asset and reputation preservation will benefit greatly from the research and valuable recommendations found in this insightful paper.”

– Bob Chaput, CEO and Founder, Clearwater Compliance LLC

“Every organization in the health care ecosystem needs to implement safeguards and controls to protect PHI and minimize financial, reputational, and legal ramifications. This report provides an invaluable five-step method for strengthening privacy and security programs that will help significantly reduce the probability of a breach.

“CISOs, CIOs, and IT security at every health care organization should have this publication in their hands today!”

– Michael Hall, CISO, DriveSavers Data Recovery, Inc.

“Health care is one of the most-breached industries. Health care providers and supporting organizations don’t currently have sufficient security and privacy budgets, including adequate processes and resources, to protect sensitive patient data. This report will help them understand what they need to do to augment their efforts.”

– Dr. Larry Ponemon, Chairman and Founder, Ponemon Institute