Health Informatics

Practical Guide

Seventh Edition

Robert E Hoyt

William R Hersh

Endorsed by

AMIA

INFORMATICS PROFESSIONALS. LEADING THE WAY.

Health Informatics

Practical Guide

Seventh Edition

ROBERT E. HOYT MD FACP
WILLIAM R. HERSH MD FACP FACMI
Editors

Health Informatics
Practical Guide
Seventh Edition

Seventh Edition

Disclaimer

Every effort has been made to make this book as accurate as possible, but no warranty is implied. The information provided is on an “as is” basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book. The views expressed in this book are those of the authors and do not necessarily reflect the official policy or position of any university or government.

First Edition: June 2007
Second Edition: August 2008
Third Edition: November 2009
Fourth Edition: September 2010
Fifth Edition: January 2012
Sixth Edition: January 2014

Print copy ISBN: 978-1-387-64241-0
eBook ISBN: 978-1-387-82750-3

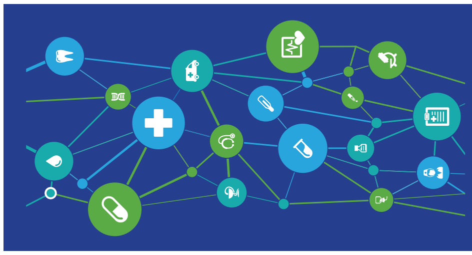
Editors

ROBERT E. HOYT MD, FACP

Diplomate, Clinical Informatics, American Board of Preventive Medicine
Informatics Education
www.informaticseducation.org
Pensacola, FL

WILLIAM R. HERSH MD, FACP, FACMI

Diplomate, Clinical Informatics, American Board of Preventive Medicine
Professor and Chair, Department of Medical Informatics & Clinical Epidemiology
Oregon Health & Science University
www.billhersh.info
Portland, OR



Contributors

ELMER V. BERNSTAM MD, MSE

Associate Dean for Research
School of Biomedical Informatics
Reynolds and Reynolds Professor of Biomedical Informatics
Professor of Internal Medicine
The University of Texas Health Science Center
Houston, TX

HARRY B. BURKE MD, PHD

Professor of Medicine
Chief of Section of Safety, Quality and Value
Biomedical Informatics
Uniformed Services University of the Health Sciences
Bethesda, MD

TREVOR COHEN MD, MBCHB, PHD

Associate Professor of Biomedical InformaticsMD
School of Biomedical Informatics
The University of Texas Health Science Center
Houston, TX

BRIAN E. DIXON MPA, PHD, FHIMSS

Associate Professor, Department of Epidemiology, IU Richard M. Fairbanks School of Public Health
Research Scientist, Center for Biomedical Informatics
Regenstrief Institute Inc.
Indianapolis, IN

ALISON FIELDS BS MPH

College of Health
University of West Florida
Pensacola, FL

M. CHRIS GIBBONS MD, MPH

Johns Hopkins Medical Institutions
Greystone Group, Inc
Baltimore, MD

JOHN GRIZZARD MD

Associate Professor, Radiology
Director, Non-Invasive Cardiovascular Imaging
Virginia Commonwealth University
Richmond, VA

WILLIAM HERSH MD, FACP, FACMI

Professor and Chair, Department of Medical Informatics & Clinical Epidemiology
School of Medicine
Oregon Health & Science University
Portland, OR

ROBERT HOYT MD, FACP

Diplomate, Clinical Informatics
Informatics Education
Pensacola, FL

TODD JOHNSON PHD

Professor, School of Biomedical Informatics
University of Texas Health Science Center
Houston, TX

HAROLD LEHMANN MD, PHD

Director, Division of Health Sciences Informatics
Professor of Health Sciences Informatics
Johns Hopkins University School of Medicine
Baltimore, MD

STEVE MAGARE MSC

Research Officer, Health Informatics
KEMRI-Wellcome Trust Programme
Nairobi, Kenya

SARITA MANTRAVADI PHD, MS, MPH, CPH, CHES

Pearland, TX

GLEBER NELSON MARQUES PHD, MS

Adjunct Professor of Computational Science
College of Health Sciences and Medicine
Mato Grasso State University
Mato Grasso, Brazil

THOMAS MARTIN PHD

Assistant Professor and Graduate Program Director
College of Public Health
Temple University
Philadelphia, PA

KEN MASTERS PHD

Assistant Professor of Medical Informatics
Medical Education Unit
College of Medicine & Health Sciences
Sultan Qaboos University
Sultanate of Oman

VISHNU MOHAN MD, MBI, MBCS, FACP

Associate Professor of Medical Informatics, General Internal Medicine and Management
Department of Medical Informatics and Clinical Epidemiology
Program Director, Clinical Informatics Sub-Specialty Fellowship
Oregon Health & Science University
School of Medicine
Portland, OR

NAOMI MUINGA MSC

Research Officer, Health Informatics
KEMRI – Wellcome Trust Programme
Nairobi, Kenya

CHRIS PATON BMBS, BMEDSCI, BMA, FACHI

Group Head for Global Health Informatics at the Centre for Tropical Medicine
University of Oxford
Oxford, England

SAURABH RAHURKAR BDS, DRPH

Public Health Informatics Postdoctoral Fellow
Center for Biomedical Informatics
Regenstrief Institute
Indianapolis, IN

JOHN RASMUSSEN MBA

Chief Information Security Officer
MedStar Health
Columbia, MD

INDRA NEIL SARKAR, PHD, MLIS, FACMI

Associate Professor of Medical Science
Center for Biomedical Informatics
Brown University
Providence, RI

YAHYA SHAIHK MD, MPH

Johns Hopkins Medical Institutions
Greystone Group, Inc.
Baltimore, MD

JOHN SHARP MSSA, PMP, FHIMSS

Director, Personal ConnectedHealth Alliance
HIMSS Innovation Center
Cleveland, OH
Adjunct Faculty, Health Informatics
Kent State University
Kent, OH

DALLAS SNIDER PHD

Assistant Professor, Computer Science
Hal Marcus College of Science and Engineering
University of West Florida,
Pensacola, FL

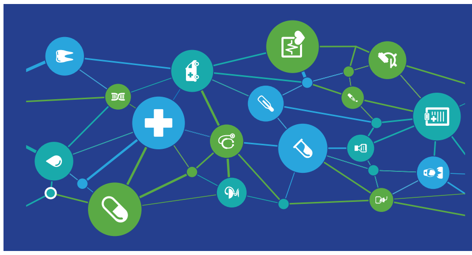


Table of Contents

Preface to the Seventh Edition

The seventh edition comprises many of the chapters included in the sixth edition and supplement with new content in each chapter and multiple new authors. We are honored to have Dr. William Hersh from Oregon Health & Science University as co-editor of this edition and he will assume the role of primary editor of all future editions. He is also a contributor of multiple chapters in the seventh edition.

We will continue the same overall chapter framework. Chapters will begin with learning objectives, followed by an introduction and history of the subject and conclude with challenges/barriers, resources, recommended reading, future trends, key points, conclusions and references. In the seventh edition, we will focus on post-HITECH Act changes in Health Informatics and other interesting developments in the field that have occurred since we published the sixth edition four years ago.

Several new authors have been added to the existing authors. The chapter on electronic health records was co-authored by Dr. Vishnu Mohan from the Oregon Health & Science University. Brian Dixon from Regenstrief Institute authored the chapter on public health informatics. Tom Martin from Temple University co-authored the chapter on telemedicine. John Rasmussen is the new author of the Privacy and Security chapter and Harry Burke is the new author of the chapter on patient safety, quality and value.

The editors and authors have provided the most up-to-date and pragmatic information about health informatics based on the continuous review of medical and lay (grey) literature. The approach taken by the editors and authors is consistent with applied informatics and not theoretical informatics. The textbook is intended to be an expansive review of the field of health informatics that will appeal to both undergraduate and graduate students in multiple fields.

Information for instructors: On our website www.informaticseducation.org we provide information about how to purchase the textbook in its many formats. Under the “Instructor’s” tab we explain that instructors can receive a PDF textbook download after registering. If they supply the university course number for the course requiring the textbook, we will also provide access to the PowerPoints and Instructor Manual. The Instructor Manual includes the following sections: background, learning objectives, chapter outline, teaching recommendations, student exercises and sample questions. Sign up for our newsletter under the “About Us tab to learn about any new textbook developments.

Information for students: All chapters include an extensive bibliography section and many chapters have a recommended reading section. In addition, we include web resources in each chapter for supplemental education.

We appreciate feedback regarding how to make this book as user friendly, accurate, up-to-date and as educational as possible.

Robert E. Hoyt MD FACP
William R. Hersh MD FACP FACMI

Acknowledgements

We would like to thank our associate editor Ann Yoshihashi MD for her many contributions to help launch the seventh edition. Without her hard work and dedication, the seventh edition would be just a notion on the drawing board.

We would also like to thank Ghislain Viau of Creative Publishing Book Design for his textbook preparation, design and formatting expertise. info@creativepublishingdesign.com

10

Health Information Privacy and Security

JOHN RASMUSSEN

LEARNING OBJECTIVES

After reading this chapter the reader should be able to:

- Explain the importance of confidentiality, integrity, and availability as it pertains to health information privacy and security
- Describe the regulatory environment and how it drives information privacy and security programs within the health care industry
- Recognize the importance of data security and privacy as related to public perception, particularly regarding data breach and loss
- Identify different types of threat actors and their motivations
- Identify different types of controls used and how they are used to protect information
- Describe emerging risks and how they impact the health care sector

INTRODUCTION

Information security and privacy have changed immeasurably during the last 15 years. Prior to the year 2000 the motivation of the computer hacker was mainly directed toward intruding into systems and acquiring data for bragging rights. When criminals determined that there was financial opportunity to be had by stealing data and controlling systems, the game had changed.

Opportunities abound in the healthcare space for individuals with malicious or criminal intent. Information systems at hospitals, insurance and pharmaceutical companies, medical device manufacturers, and small provider practices are an inviting and rich target for these individuals. The data maintained by the health care industry can be personally identifiable, clinical, financial, and valuable intellectual property.

This chapter will explore the foundational elements of information security and describe the regulatory environment that is driving the healthcare sector to implement controls to protect data. It will demonstrate the types of breaches that have occurred, and risks associated with the breach of information. The chapter will also describe the different types of controls and their application to help prevent security and privacy incidents from occurring. In addition, individuals who work within healthcare play an important role in securing information and this chapter will describe how they can help. Finally, the chapter will discuss emerging risks to information security and privacy within healthcare.

BASIC SECURITY PRINCIPLES

Electronic information is everywhere. As technology spreads and new technologies develop, the healthcare sector faces many new challenges in protecting the security and privacy of that data. The increased adoption of electronic health records, coupled with personal health records and health information exchanges creates some monumental challenges in the coordination of protection for that data. How does a hospital, clinic, or insurance company secure the most sensitive personal data of individuals and still maintain the ability to use that information for the provision of quality care to the patient?

Some 2013 findings indicate that a little over 12% of participants had withheld information from a healthcare provider because of security concerns.[1] This lack of communication could have dire consequences on the provider/patient relationship and essentially the patient's health as a whole. But without better assurances and solutions by vendors, insurers and health care organizations, it may be difficult to win and keep the public trust.

To understand health information privacy and security it is important to understand the discipline of information security through some basic concepts and to understand where privacy lands as part of that discipline. This section covers some basic security principles and describes how those principles apply to privacy.

Data Classification and Privacy

Information stored, transmitted, or created by electronic systems can come in many flavors. One component of that information can be elements of personal data that can be construed as sensitive information. Any company dealing with data will have a data classification policy that determines the sensitivity of data and how that organization may choose to protect it.

A data classification program should be broken down by Security Objective and Potential Impact if that data is compromised.[2] The Federal Information Processing Standards (FIPS), Standards for Security Categorization of Federal Information and Information Systems (FIPS PUB 199) presents a guideline for classifying data through the Security Objectives (confidentiality, integrity, or availability) to determine if the Potential Impact is low, medium, or high. Once Impact is determined, proper controls can be put into place. There are many different factors that contribute to the impact ranking, including specific data elements and regulatory requirements to protect that data.

There are a myriad of regulatory requirements dealing with the protection of confidential information and protecting the privacy of individuals whom the data references. Those regulations will be discussed later in this chapter.

The privacy of health data falls squarely in the "confidentiality" Security Objective. There are many elements of health data that would be considered sensitive or harmful to the subject of the information if it is accessed, used, or disclosed in an unauthorized manner. Examples of sensitive data elements include Social Security Number, credit card number, sensitive diagnosis, family medical history, etc.

Confidentiality, Integrity, and Availability

According to the International Information Systems Security Certification Consortium (ISC2), among others, there are three pillars of information security (confidentiality, availability, and integrity) that are fundamental to protecting information technology solutions such as health information technology (HIT). In FIPS they are also referred to as "Security Objectives."[3]

Security measures are instituted collectively to meet one or more of these primary goals, with the result being one where confidentiality, availability and integrity are all covered. These terms are ubiquitous in the practice of information security across all industries. Whether in banking, manufacturing, or healthcare, these terms are commonly used when developing and maintaining information security programs.

- Confidentiality refers to the prevention of data loss, and is the category most easily identified with HIPAA privacy and security within healthcare environments. Encryption, access control, and secure authentication are typical controls used to protect confidentiality.
- Availability refers to system and network accessibility, and often focuses on power loss or network connectivity outages. Loss of availability may be attributed to natural, accidental, or intentional disasters. Natural disasters can include tornados, earthquakes, hurricanes or fire. Accidental incidents such as the loss of a personal thumb drive, misconfiguration of a system, or a backhoe digging up a fiber optic cable are the most common availability issues. Availability can also be impacted by individuals or groups intentionally attacking systems or data. These attacks can include denial of service attacks (DoS) which target an organization and bombard it with data until legitimate data can no longer be received, or through ransomware which infects a computer with a virus that will encrypt the user's data until a ransom is paid. To address the risk to availability organizations will use redundant systems, backup batteries and generators, separate data centers, and data backups to protect their data.
- Integrity describes the trustworthiness and permanence of data, an assurance that the lab results or personal medical history of a patient is not modifiable by unauthorized entities or corrupted by a poorly designed process. Database best practices, data loss solutions, and data backup and archival tools are implemented to prevent data manipulation, corruption, or loss; thereby maintaining the integrity of patient data. Organizations also use audit logging for access to systems and databases as a means of protecting the integrity of the data. One strategy employed by hackers is to delete audit logs of systems they intrude upon, thus erasing any evidence of changes they made to the system.

Defense in Depth

With the protection of confidentiality, integrity, and availability as key objectives, and with the help of data classification to know what is important to protect, the organization must then develop a set of controls to protect its data. In most cases one control will not be adequate to protect the data. An organization must employ several different kinds of controls to protect its data from compromise. Building several layers of security controls around data is often referred to as "Defense in Depth."[4]

This concept acknowledges that one layer of defense may not be able to contain the risk to data being compromised and by adding additional layers the level of risk can be reduced significantly. A common analogy to describe this concept is that of a castle. The castle is usually built in a strategic location with a wide plane of view, so the inhabitants can see any threat from far off and enact other defenses. Once the attacker gets close enough to the castle they are in danger from arrows reaching far beyond the walls. If the attacker gets close to the castle they will have to cross a moat and then scale the walls or breach the front gate of the castle. If the attacker is fortunate enough to get over the first wall it is likely that they will see additional walls and additional defensive objects, each more difficult to overcome. While not foolproof, this defensive strategy will make the attacker think twice about the costs associated with attacking the castle.

Healthcare organizations will use a combination of technical, administrative, and physical safeguards to protect their systems and information. Each of these may have additional controls in place to further reduce risk.

An example of defense in depth in healthcare:

1. A healthcare organization has a set of policies and procedures around data privacy and security that the employee receives training on and acknowledges annually – Administrative Safeguard
2. New employees are given a criminal background check, drug screen and credit check prior to employment – Administrative Safeguard
3. The new employee is given a badge with their photo and the ability to access restricted areas through a proximity sensor – Physical and Technical Safeguard
4. Each employee has their own user name and password to access the entities electronic resources – Technical Safeguard
5. Access is given to only the systems that the employee needs to access, minimum necessary – Technical and Administrative Safeguard
6. The computer that the employee uses is encrypted, has patches automatically pushed to the device, and runs anti-virus software – Technical Safeguard
7. The email system the employee accesses has anti-virus installed on the server, has patches updated by the technology team, and is encrypted. It also uses an email gateway to filter out spam, phishing (this is a social engineering technique that tricks the individual into taking an action like clicking on a malicious link, downloading an attachment, or providing their credentials), and emails containing known malware – Technical Safeguard
8. The network that the email system, and computers operate on is located behind a firewall, intrusion prevention system, and switches and routers which employ access control lists (ACLs) to limit the types of traffic allowed on the network – Technical Safeguard.

The examples above are very high-level examples of the controls applied to the healthcare environment. These are standard techniques that start with the individual (these controls are also applied to patients and visitors) and work their way all the way up the technical stack to data centers and the Internet.

THE HEALTHCARE REGULATORY ENVIRONMENT

The healthcare industry is a heavily regulated industry. Given the nature of the enterprise it is not surprising that state, federal, and industry actors want a stake in protecting the safety of the patient population. This section will provide an in-depth review of the Health Insurance Portability and Accountability Act (HIPAA) and identify other industry standards and regulatory requirements as they pertain to healthcare privacy and security.

HIPAA

HIPAA was originally created to promote the portability of health insurance but gained additional prominence as the key regulation affecting the industry by including requirements to protect patient privacy and fulfill certain patient rights. In the 20 years since its passage it has evolved and been updated to reflect new threats and to provide clarification and interpretation to language that has been part of the law. Updates came in the form of the Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act of 2009.

HITECH imposed new requirements for breach notification and imposed stiffer penalties for non-compliance with HIPAA.[5] In addition, it added new patient rights to HIPAA.

The HIPAA Privacy and Security Rule (45 CFR Parts 160, 162, and 164) is enforced by the Office for Civil Rights (OCR), which operates under the Office of the Secretary of the Department of Health and Human Services.[6] The OCR began enforcing HIPAA in 2003. Their enforcement actions include the investigation and resolution of patient privacy complaints as well as investigation of breaches of protected health information (PHI).

First and foremost, HIPAA only applies to organizations defined as "covered entities."[7] If an organization does not meet the definition of a covered entity then it is not subject to the law. Types of organizations that *do not* have to follow HIPAA include but are not restricted to the following: independent research organizations, life insurers, employers, many school districts, many law enforcement agencies, and worker's compensation carriers.

Covered entities include:

- Health Plans – which includes health insurers, HMOs, company health plans, and government programs such as Medicare and Medicaid.
- Healthcare clearinghouses
- Healthcare Providers – which includes most doctors, clinics, hospitals, psychologists, chiropractors, nursing homes, pharmacies, and dentists "who transmit any health information in electronic form in connection with a transaction covered by this subchapter" (45 CFR § 160.102). This means the provider must transmit data between two parties to "carry out financial or administrative activities related to health care." 8 For example, a dentist submitting a billing claim to an insurance carrier would meet this definition. If a provider does not meet this definition, i.e. only takes cash payment and does not conduct any "transaction" as defined in HIPAA, ("Transaction means the transmission of information between two parties to carry out financial or administrative activities related to health care"), they are not considered a covered entity and therefore not subject to HIPAA.

For those organizations that are required to abide by HIPAA, patient data and personal information must be protected according to the Security Rule. Protections apply to all protected health information (PHI), whether in hard copy records, electronic protected health information (ePHI) stored on computing systems, or even verbal discussions between medical professionals. Covered entities must put safeguards in place to ensure data is not compromised, and that it is only used for the intended purpose. The HIPAA rules are not designed to and should not impede the treatment of patients.[9]

Covered entities must comply with certain consumer rights. Specifically, a patient may:

- Request and receive a copy of their health records
- Request an amendment to their health record
- Receive a notice that discusses how health information may be used and shared, the Notice of Privacy Practices
- Request a restriction on the use and disclosure of their health information
- Receive a copy of their "accounting of disclosures"
- Restrict disclosure of the health information to an insurer if the encounter is paid for out of pocket
- File a complaint with a provider, health insurer, and/or the U.S. Government if patient rights are being denied or health information is not being protected.10

Protected Health Information (PHI)

The term Protected Health Information is defined as "*individually identifiable health information*" with some exclusions. Breaking this down, individually identifiable health information is:

- Information created by a covered entity
- And "relates to the past, present, or future physical or mental health or condition of an individual"
- Or identifies the individual or there is a reasonable basis to believe that the individual can be identified from the information.11

The first elements and one of the other two elements must be present to be considered PHI.

Permitted Uses and Disclosures of PHI

HIPAA allows covered entities to use or disclose PHI for treatment, payment, or healthcare operations. "Use" refers to the internal use of PHI within an organization and "disclosure" refers to the release of information outside of the organization. These uses and disclosures are limited to the "*minimum necessary*" to prevent misuse or to protect privacy.[12]

For example, a health system may have two software programs for their electronic health record, one which contains treatment notes and the other billing information. When applying the concept of "*minimum necessary*" a doctor would have access limited to the treatment notes and a billing specialist would be limited to access to the billing system used by the hospital.[13]

Covered Entity Permitted Uses and Disclosures of patient data according to the Privacy Rule:

- To the individual
- For treatment, payment or health care operations
- Uses and disclosures with opportunity to agree or object
  o Facility directories
  o For notification and other purposes
- Public interest and benefit activities
  o Required by law
  o Public health activities
  o Victims of abuse, neglect or domestic violence
  o Health oversight activities
  o Judicial and administrative proceedings
  o Law enforcement purposes
  o Decedents
  o Cadaveric organ, eye, or tissue donation
  o Research
  o Serious threat to health or safety
  o Essential government functions
  o Workers' compensation
- Limited data set – this can include health information and dates; no other individual identifiers are included in a limited data set
- De-identified data – this is data where all individually identifiable information has been removed.14

The 18 individual identifiers named in the rule include:

1. Names
2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP Code, and their equivalent geographical codes, except for the initial three digits of a ZIP Code if, according to the current publicly available data from the Bureau of the Census:
   a. The geographic unit formed by combining all ZIP Codes with the same three initial digits contains more than 20,000 people.
   b. The initial three digits of a ZIP Code for all such geographic units containing 20,000 or fewer people are changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
4. Telephone numbers
5. Facsimile numbers
6. Electronic mail addresses
7. Social security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web universal resource locators (URLs)
15. Internet protocol (IP) address numbers
16. Biometric identifiers, including fingerprints and voiceprints
17. Full-face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code, unless otherwise permitted by the Privacy Rule for re-identification[15]

The Business Associate

Not all services can be managed by a hospital or clinic. Some services may need to be outsourced to a partner who has the expertise that the healthcare entity does not have in-house. Some of these partners or vendors will need to view, access, process, or create PHI on behalf of the covered entity. These organizations would then become a Business Associate (BA) to the Covered Entity (CE). Business associates can be an electronic health record (EHR) software company, a third party that assists with billing and claims, or a transcription service.[16]

A BA is required to have a business associate agreement (BAA) in place with the CE under HIPAA. The BAA ensures that the BAs meet the requirements of the Security Rule under HIPAA and places the proper protections around PHI. A BA is also responsible for obtaining BAAs with any other organizations that sub-contract to it and those organizations are also required to follow the Security Rule. This cascades the responsibility of protecting PHI to all of the vendors and sub-contractors who work with that information. This requirement was added to HIPAA as part of the HITECH Act as was the ability for the OCR to enforce HIPAA among business associates. The business associate can now be penalized for violating HIPAA through civil action by the OCR and criminally by the Department of Justice.[17]

The Security Rule

HIPAA requires that covered entities apply safeguards to protect patient information. There are three categories of safeguards identified in HIPAA that have different sets of "required" and "addressable" controls. All required controls must be put in place. An addressable control is one that is also required, however, compensating controls can be used if the addressable control is not available to the covered entity. HIPAA takes into account the ability of a covered entity to apply safeguards based upon their size and financial position and allows for a "*flexibility of approach*" in order for the covered entity to meet the security requirements of the Security Rule.[18]

Safeguard areas and examples of controls:

- Administrative Safeguards – policy or procedures used to provide security and governance to privacy and security.
  - o Security management processes to reduce risks and vulnerabilities
  - o Security personnel responsible for developing and implementing security policies
  - o Information access management - minimum access necessary to perform duty
  - o Workforce training and management
  - o Evaluation of security policies and procedures
- Physical Safeguards – physical security measures taken to protect information. Typically, they are in the form of locks, security cameras, guards, or badge access to restricted areas.
  - o Facility access and control limiting physical access to facilities
  - o Workstation and device security policies and procedures covering transfer, removal, disposal, and re-use of electronic media
- Technical Safeguards – technical tools implemented to protect data. These can be firewalls, anti-virus, automatic logoff, session timeouts, intrusion detection, or a wide variety of other technical controls.
  - o Access control that restricts access to authorized personnel
  - o Audit controls for hardware, software, and transactions
  - o Integrity controls to ensure data is not altered or destroyed
  - o Transmission security to protect against unauthorized access to data transmitted on networks and via email[19]

Breach Requirements under HIPAA

Subpart D, 45 CFR 164.4XX of HIPAA deals entirely with the breach of protected health information and was added as a result of the HITECH Act to strengthen the privacy protections of HIPAA and outline the requirements for breach notification.

A "breach" is a complicated thing to define. Simply, a breach is an unauthorized acquisition, access, or use of PHI with a number of exceptions.[20]

Exceptions:

1. Data is encrypted. This is considered a safe harbor; or
2. "*Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure*"; or
3. "*Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed*"; or
4. "*A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.*"[21]

If the incident does not meet one of the exceptions above a breach risk assessment must be done to determine if the incident exceeds a low probability of compromise. This is determined by looking at four factors together:

1. The nature and extent of the PHI involved. A sensitive diagnosis or the release of a Social Security Number would exceed a low probability for this factor.
2. The person who used the information or who it was disclosed to. If an employee stole PHI for personal gain this would exceed low probability for this factor.
3. Whether the PHI was actually acquired or viewed. A laptop containing PHI, if unencrypted, is considered "acquired" and would exceed low probability for this factor.
4. The extent to which the risk to PHI has been mitigated. If email is sent to an unauthorized individual and no attempt is made to retrieve or delete the email, this would exceed low probability for this factor.[22]

If a breach is determined, the covered entity must notify the individual(s) impacted by the breach. They must inform them within 60 days of when the breach is identified. The notification must include:

- A description of what happened
- A description of the type of PHI that was breached
- Steps the individual can take to protect themselves
- What the covered entity is doing to investigate the breach and mitigate harm

- Contact information for the individual to contact the covered entity23

If a breach exceeds 500 individuals, the covered entity must notify the media and must report the breach to the Office for Civil Rights (OCR).

Regardless of the number of individuals impacted by a breach, all breaches must be reported to the OCR annually.[24]

OTHER REGULATIONS AND HEALTHCARE PRIVACY AND SECURITY

While HIPAA is the best known regulatory requirement affecting healthcare, there are a number of other regulations or industry standards that deal with privacy and security protections. Table 10.1 outlines security standards and laws.

BUSINESS DRIVERS FOR SECURITY AND PRIVACY

In addition to the regulatory requirements governing privacy and security within healthcare, the business must calculate cybersecurity as part of its overall risk profile. Healthcare entities are very familiar with calculating the risk of medical malpractice as litigation for malpractice can cost millions to an organization and harm their reputation. As more and more technology is introduced into the healthcare space there is more opportunity for risk that must be considered as part of doing business. Cybersecurity concerns are foremost of these concerns as they can harm the patient, visitors, or employees of a healthcare entity.

A heavy fine from a regulatory entity can impact the reputation of an organization. The OCR has a website known as the "*Wall of Shame*" which shows all breaches currently under investigation and a second site that shows all "*Resolution Agreements*."[25-26] These sites are easy for consumers and media to reference when they want to call attention to a certain entity and can have an impact on the reputation of that entity, though it is very difficult to measure the impact on reputation.

Another business driver for healthcare is loss of market share or value. This ties directly to reputation but is not dependent upon a negative reputational impact. One example of this occurred in 2016 when a short selling financial firm named Muddy Waters bought information about a security vulnerability in a pacemaker produced

Table 10.1: Security Standards and Laws

Security Standard/Law	Brief Description
ISO 20000/27000	International IT Governance and IT Security standards
COBIT	IT Governance framework
ITIL	Information Technology Infrastructure Library, IT service management
NIST SP 800-53	National Institute of Standards and Technology, IT security controls
SOX	Sarbanes–Oxley Act; Public company accounting law
PCI-DSS	Payment Card Industry Data Security Standard – applies to all credit card merchants
FISMA	Federal Information Security Management Act
FERPA	Family Educational Rights and Privacy Act – applies to student records. If a covered entity is also an academic medical center, student health records would be protected under this regulation
State Laws	Almost every state in the United States has laws that require notification in case of a breach. If a covered entity has patients in several different states it will need to consider the breach notification laws for each state if there is an incident involving patients who reside in those states
GDPR	General Data Protection Regulation – this is a European Union regulation that requires companies that process personal information for EU citizens, including medical data, to protect that data.

by St. Jude Medical Inc. from a cyber security firm named MedSec Holdings Inc. and then shorted the stock before publicly disclosing the vulnerability. The announcement caused St. Jude shares to fall by 4.96 percent in one day, also producing a 7.4 percent discount to Abbott Laboratories which was working to acquire St. Jude.[27]

To respond to these risks insurance companies have been building new products that address these concerns or working to modify existing products, so they can fill the needs of this new risk area. Companies like Beazley offer breach response insurance packages that include coverage for notification to individuals impacted by the breach, fines and corrective actions, or incident response.[28]

Privacy And Security Roles And Governance In The Healthcare Organization

Information privacy and security are evolving in organizations as their role becomes more and more important. The roles of Information Security Officer and Privacy Officer are identified in HIPAA as a requirement for covered entities.

The top positions for security are typically called Chief Information Security Officer (CISO) and Chief Privacy Officer (CPO). Their reporting relationships can differ depending on an organization's size, industry, compliance mandates and laws, technology initiatives, maturity, private or public status, and even profit model.

In some models the CISO and CPO report to the Chief Compliance Officer or Chief Risk Officer of an organization.

Other models have a Chief Security Officer role that reports directly to the president of an organization and has a CISO and CPO that report directly to them.

The most common model is to have the CPO report to a Chief Compliance Officer and the CISO report directly to the Chief Information Officer (CIO).

Information security policy is usually established under the direction of the CIO, but it is more common to see an information security committee chartered with the responsibility of creating these policies. Likewise, privacy policies are usually established under the Chief Compliance Officer but can be driven by a committee.

Depending on resources, the information technology teams may consist of network, system administration, security and data personnel, or could be the very same technical staff relied upon for all office or clinic IT needs. No matter the titles, this supporting staff is often tasked to defend key systems, networks, and patient data from risk, and assist with any investigations resulting from a data breach.

BREACHES IN THE NEWS – AND CONSEQUENCES

Healthcare data breaches are frequent and with the strengthening of penalties under the HITECH Act they make a big splash when they hit the news. While the examples listed below may list the financial consequences of a violation of regulatory requirements, they are not inclusive of the costs of a corrective action plan (CAP) which usually accompanies a civil penalty or settlement with the OCR. These costs can be many times higher than the actual penalty as an entity must apply expensive technology to their environment, hire additional security and compliance staff, rewrite policy, and retrain staff all within the window defined under the CAP.

- Advocate Medical Group (2013/2016) – In July 2013, Advocate reported that patient health and identity data for 4 million patients was at risk due to theft. The data were contained on 4 unencrypted company computers stolen from their administrative building and contained names, addresses, birth dates and personal health data. While this is historically the second largest breach, what is most notable is that this is their second large breach (over 500 patients).29 Less than a month after the announcement of this breach there were two class action lawsuits addressing Advocate's "failure to take the necessary precautions required to safeguard patients' protected health information" and claiming that the computers were stolen from an "unmonitored" room with "little to no security."30 The suits also cite negligence, invasion of privacy, consumer fraud, and intentional infliction of emotional distress. 31 The OCR settled the investigation with Advocate in 2016 when Advocate agreed to pay the settlement amount of $5.55 million and adopt a corrective action plan. This is the largest settlement to date.
- Oregon Health & Science University (OHSU), (2013/2016) – In March of 2013 OHSU experienced a breach when an unencrypted laptop was stolen from a surgeon who was on vacation in Hawaii. The laptop contained information for over 4000 patients, including surgery schedules. Notification was provided to the individuals affected.32 Later that year a second breach notification was sent out to an additional 3000 patients for a disclosure of PHI on Google Drive by residents who were using these services to keep a spreadsheet of patients.33 Since there was no business associate agreement in place with Google, the breach notification was required.

These incidents, occurring in the same year, led to the finding by the OCR that OHSU did not perform adequate risk analysis and apply timely controls to mitigate risk. OHSU settled for $2.7 million and a three-year corrective action plan.34

- TRICARE (2011/2014) - The largest breach in history occurred in 2011 and was reported to have affected between 4.9 and 5.1 million military active duty service members, retirees, and their families within the TRICARE health system.35-36 The breach was in the form of unencrypted backup tapes stolen from the vehicle of an employee of Science Applications International Corp (SAIC), a TRICARE contractor.37 The data was expansive and covered those cared for in military facilities between 1992 and September 2011. Information that was contained on the tapes included names, addresses, birth dates, social security numbers, and personal health data. There was no financial data such as credit card or bank account information contained on the tapes; however, with the level of personal information that was obtained financial ramifications have been reported by the affected patients. Four people initially filed a single $4.9 billion federal lawsuit against TRICARE and SAIC in 2011, but by the close of 2012 the suits grew to eight that were consolidated into one to be heard and handled by the U.S. District Court in Washington, D.C. On May 9th, 2014, the U.S. District Court in Washington, D.C. threw out most of the case stating that it was "speculative" that the plaintiffs may suffer harm from the breach.38 This illustrates one a challenge with the multitude of breaches of personally identifiable information, that it is very hard to prove that harm, damage, or loss was a direct result of the breach.
- Affinity Health Plan, Inc. (2010/2013) – This breach occurred in 2009 but went unreported until 2010 and affected more than 300,000 patient records. While not the most significant in terms of novelty or number of records, the distinguishing feature of this breach is how the data was breached. Affinity had returned seven photocopy machines they had leased long term. Unfortunately, the copiers were then sold to media giant CBS News as part of an investigative report on data security risks. The units had not been wiped before return and confidential patient information remained on their storage hard drives. Three hundred pages of documents from one copier contained personally identifiable information and included sensitive medical test results, cancer diagnoses, and prescription drug information.39 In August of 2013, the U.S. Department of Health and Human Services (HHS) announced a settlement agreement that included a fine of over $1.2 million and a Corrective Action Plan (CAP) that required Affinity to use its best efforts to obtain all hard drives from previously leased machines and to take specific measures to safeguard their patient's health information.40 This story highlights the importance of understanding the comprehensive nature of patient health data storage and exploring non-traditional avenues through which breaches may occur.

THREAT ACTORS AND TYPES OF ATTACKS

It is important to understand the different types of threat actors and their motivations to understand why information from the healthcare industry is targeted. The actors identified below have malicious intent. It is also important to note that an additional threat, albeit inadvertent, to the environment is the individual employee. The regular employee can accidentally initiate a security incident through misuse of computer resources, like visiting a malicious webpage and downloading malware, or they can cause downtime through improperly following change control processes. Some information technology employees may try to initiate a change to the configuration of a system in the production environment without first testing the change in a test instance and creating a back out plan if the change fails. This can lead to all manner of availability issues and can extend the downtime if the change was not formally documented and there is a need to systematically troubleshoot the problem.[41]

- Insiders – these are employees or other individuals within the organization who have direct access to electronic resources.
  - o Motivation – financial gain, or revenge.
  - o Consequences – these individuals may steal information to resell it or to build their own information. If financial gain is their goal they will target business confidential information or intellectual property. The individual may also hold a grudge against the organization for some perceived or real slight against them. In this case, the individual may be out to cause damage to the organization by deleting information, sharing information without authorization, or causing damage to electronic systems.[42]
- Hacktivists – these are individuals or groups who do not have direct access to the organization's electronic resources.

- o Motivation – hacktivists usually have a grudge or political agenda against the organization.
- o Consequences – they are out to disrupt business or to embarrass the organization. They will deface websites or publicly post personal information about employees to spur additional action and draw attention to their cause.[42]

- Organized Crime – the most common and high profile of all threat actors.
  - o Motivation – financial gain.
  - o Consequences – the goal of organized crime is to earn money from their activities. This is a low risk – high reward endeavor as many countries will not extradite individuals who are accused of stealing data or money. One grand example of a cyber heist is the $81 million theft from the Bangladesh Bank on February 4, 2016.[42-43] Hackers used credentials stolen from 4 employees to initiate transfers to banks in the Philippines. The attack was disrupted and $850 million in additional transfers were stopped. This is an extreme example of organized crime, more commonly these criminals are trying to get smaller payouts by targeting individuals with schemes like Nigerian 219 emails where the individual receives an email from an exiled leader and can receive millions of dollars if they can help that leader transfer money out of a bank where it is held.[44]
- Nation States – can be nation states or hackers sponsored by nation states.
  - o Motivation – national interest, espionage, cyber warfare, financial gain.
  - o Consequences – Nation States are the most nefarious of threat actors because they have the full power and financing of the nation behind their activities. They are out to seek advantages in the international arena through any means necessary and may be responsible for some very costly attacks. If espionage or theft of intellectual property is the motivation a nation state will become an "*Advanced Persistent Threat*" (APT), meaning that they will intrude on a system and lay in wait until they discover what they need.[45-46] They will be very stealthy and the victim will have no idea that the attacker is there until it is too late.
    - § Sony hack – in October 2014 Sony Pictures employees were greeted by an image of a red skeleton and the words "#Hacked by #GOP," on their login screens. The attackers stole many internal documents and other intellectual property and posted some of this information on the Internet to embarrass Sony. The attack has been attributed to North Korea and the motivation was outrage over the movie "The Interview" which depicted an assassination plot against Kim Jong Un.[47]
    - § Electric grid in Ukraine – December 2015 a cyberattack shut down the electrical grid to 250,000 Ukrainians. The attack has been attributed to Russia who had been in a state of conflict with Ukraine for years.[48]
    - § Anthem breach – in February 2015 hackers stole the information of 80 million current and former members of Anthem insurance. This personal information may have been targeted for financial gain or for espionage purposes. Personally identifiable information could be used to create new identities or sign up for financial services. Any health information, if sensitive, could potentially be used for blackmail purposes if the foreign government wanted to have some leverage over a person. It is suspected that China is responsible for this attack.[49]

Types of attacks

There are many different ways a threat actor can attack their target. This section will describe some of the methods of attack.

- Social Engineering – the weakest link in the organization is going to be the end user. Individuals susceptible to manipulation by things that seem familiar and friendly to them but are actually malicious in nature. Social engineering attacks attempt to get the end user to do something they would not normally do, thus allowing the threat actor access to their system or information. Social Engineering is the most frequently used form of attack.[50] There are many different techniques for social engineering, here are some examples:
  - o Phishing - typically in the form of email but can also come in a telephone call or text message, that poses as a legitimate person or institution in order to lure the victim into giving away sensitive information like usernames, passwords, or financial information. They can also lure the victim to download and install malware on their computer or phone. Phishing may also:
    - § May appear to come from someone you know or your place of work
    - § Displays a sense of urgency, such as "invoice overdue"
    - § Appears to be too good to be true

§ Could contain hyperlinks or attachments leading to fake login pages or posing as legitimate documents.[51]

o Shoulder surfing - the attacker merely looks over the victim's shoulder and views restricted information or copies down their password.

o Tailgating - the attacker uses someone else's access to a restricted area by following closely behind the individual who has already used their ID badge to unlock access to that area.

o The promise of free hardware - there is no regular term for this, but it is a highly effective form of social engineering where a threat actor will leave USB sticks seeded in a parking lot or laying on a counter for an unsuspecting employee to pick up. If the employee picks up the USB, plugs it in and clicks on a file on the drive they could infect their machine with malware. One study by Google's anti-abuse research team discovered that 98 percent of 297 dropped USB sticks were picked up and those individuals clicked on files on 45 percent of those recovered sticks.[52]

Other direct attacks that do not involve social engineering, but may occur as the result of successful social engineering attacks include:

- Denial of Service (DoS) - a DoS attack is intended to stop traffic from reaching a certain website or destination through flooding that site with bogus requests, so legitimate traffic cannot get through.[53] On October 21, 2016 Dyn, a company that helps route Internet traffic through management of Domain Name Service (DNS), was hit by - two massive DoS attacks. Since Dyn managed DNS for many parts of the internet the DoS attack not only brought Dyn to a standstill, it impacted traffic routed to many of Dyn's customers and slowed or stopped their traffic.[54]
- Brute Force attack - this is an attack where the threat actor will attempt to throw random credentials at an application login page to see if they can gain access. If an organization uses a strong password policy and a technical control that locks the account after a certain number of unsuccessful login attempt this type of attack can be easily thwarted. However, there are certain devices or systems that come with default passwords set up as administrators for the system. Many people do not change these default passwords so a brute force attack against this type of device can be easily successful after throwing a few passwords at the system like "admin," "password," "123password," "administrator," etc.[55]
- Doxing - this is a relatively new attack technique that has a substantial impact on privacy. Doxing gathers information about the victim and publishes that information in order to embarrass or harass the individual. The more sensitive the data, the more powerful the attack. This attack technique would be typically employed by a hacktivist.[56]

TOOLS USED TO PROTECT HEALTHCARE PRIVACY AND SECURITY

Earlier in this chapter Defense in Depth was defined. This section will describe a few of the tools and operational techniques to prevent the unauthorized access, use, or disclosure of information created or maintained by a healthcare entity. This section is by no means a comprehensive list of solutions that can be used to protect privacy and security. This is a high-level description of some of the tools that encompass the technical, administrative, and physical controls referenced in HIPAA.

There are many technical controls available to healthcare entities to employ in their defenses. These can be applied at different layers through the organization's IT infrastructure.

Client protection

- Patching: Applications and operating systems (OSs) may arrive with vulnerabilities present. These vulnerabilities can be identified through regular use or through individuals testing the software or OS. Some of these vulnerabilities can be exploited to introduce security risks. In order to reduce these risks, the vendors will patch periodically. Patches may also contain feature enhancements or bug fixes. Vendor updates may occur monthly or much less frequently. To prevent the exploitation of these vulnerabilities an organization must patch their systems or applications as soon as practical after the patch is released. The longer a system remains unpatched, the more vulnerable it becomes. Most exploits for systems utilize known vulnerabilities.
- Anti-virus: This is software developed for the computer or device that detects and blocks viruses from executing and infecting the device. Many traditional anti-virus solutions are signature based and will only work if the product is already aware of the virus. Anti-virus solutions must receive updates on a periodic basis to be effective. New variants of viruses are released daily, and the anti-virus solution must be updated as the threats change. Newer solutions of anti-virus software are called next-generation antivirus. This software catalogs system processes and uses algorithms to detect and block virus behavior.[57]

- Encryption: This technology renders information unreadable without the appropriate key to unlock that information. When applied to clients such as personal computers, laptops, or smart phones, encryption can be file-based or whole disk. File-based encryption does not touch the operating system, it encrypts each of the files on the device. Whole disk encryption renders the entire disk unreadable without the key. Both technologies are considered encryption for data at-rest, meaning that when an individual is logged in or the device is powered on the data is readable. Once the device is turned off or rebooted a key is necessary to unscramble the data.[58]

Application and database protection

- Strong authentication: Keeping applications and databases secure relies on limiting access to the system to those who are authorized to use the system and using an authentication method that proves the individual is who they say they are. Authentication methods can include a password, token, or biometric. A combination of two of these authentication methods, dual-factor authentication, can be used to strengthen the security around these systems. The factors fall into three categories – something one knows, something one has, or something that one is.[59]
  - o Password: this is the most widely used method of authentication where a user types in a password to gain access to the system. Passwords can be a PIN number like those used for ATM withdrawals or can be a longer combination of letters, numbers, and special characters.
  - o Token: a token can come in the form of a smart card, key fob, or an application on a smartphone that generates a one-time PIN number for the user to enter to access the system.
  - o Biometric: this is an authentication method that uses a part of the body to provide access. These can include retina scanning, hand geometry, and fingerprint.
- Privileged account management (PAM): used to protect accounts with elevated access to a system. These systems are meant to limit the time an elevated credential can be used to prevent these accounts being used against the organization. Software programs exist that catalog privileged accounts and change their passwords frequently. To use an administrative level password a technician would be required to log into the PAM system and check out the password they need. The password would be generated, given a short time to live, and signed out to the user.[60]
- Backup and continuity of operations: there are times when a system may become unavailable due to hardware or software failure as well as times when data may be corrupted such as during a ransomware attack. Organizations must have backup and recovery strategies in place which are regularly tested to ensure data and systems can be brought back up in a timely manner. Some organizations will employ a strategy of using several different data centers that mirror each other's data in case there is a power outage or other emergency. These data centers will have redundant power, internet connectivity, and backup power in the form of batteries and generators. Data will also be backed up at these sites to tape or disk. When data is backed up to tape it is typically stored off site, so it would not be damaged or lost if there was a fire or flood at the data center.
- OWASP: Open Web Application Security Project (OWASP) is an organization focused on improving the security of software. Application security begins with good coding and security practices built into the project.[61] OWASP identifies ten proactive controls that should be included in every software development project:
  - o Verify for Security Early and Often
  - o Parameterize Queries
  - o Encode Data
  - o Validate All Inputs
  - o Implement Identity and Authentication Controls
  - o Implement Appropriate Access Controls
  - o Protect Data
  - o Implement Logging and Intrusion Detection
  - o Leverage Security Frameworks and Libraries
  - o Error and Exception Handling[62]
- Vulnerability analysis and penetration testing: applications and systems should be checked periodically to see if new vulnerabilities have been discovered or introduced into a system. This can be done by hiring third parties to test or through the organization conducting routine tests against their own systems specially designed to identify vulnerabilities. Once identified the organization will need to develop a mitigation strategy to prevent those vulnerabilities from being exploited.[63]

Border defenses

- Firewalls: these are network devices or software products that allow or reject traffic to different network zones.[64] Firewalls can be used to define different levels of trust on different areas of the network. For example, the main database for an electronic health record system would not be directly connected to the internet. It would be protected by a firewall that would only allow certain traffic or users to access it.

- Intrusion detection: this technology is used to detect anomalies within the system or network that may not be caught by other layers of protection like firewalls or antivirus software. These solutions monitor network traffic, system logs, and system usage to determine abnormal behavior. Intrusion detection can be network based or host based to provide a more granular view of potentially harmful activity.[65]
- Web filtering: most users in an organization will have a need to access the internet as part of their work. Work policies may also allow a user to access the Internet for personal purpose. Whether for business or personal use, the Internet can be a dangerous place and protections need to be put into place to prevent the user from inadvertently infecting their workstations or allowing a threat into the organization. A web filter will catalog and block access to sites known to contain malicious software. These solutions are also referred to as "content control software" as their secondary purpose may be to limit the users from accessing sites that may not be appropriate for work such as those related to pornography, gambling, or hate speech.[66]
- Virtual Local Area Networks (VLANs): are networks that attach objects from one or more LANs in a way that makes them appear as if they are all on the same LAN. They take advantage of logical connections rather than physical connections and can assist in creating segments that help secure different areas of the network.[67] Within the healthcare environment they can be used to limit access to objects that may be vulnerable to internal or external threats. VLANs can be used to segregate biomedical devices from the rest of the network so they are less likely to be compromised.
- Encryption in transit: earlier in this section encryption for data "at rest" was described. Encryption for data in transit takes data from the source system and renders it unreadable using a set of keys and then sends the data on to its destination where the receiving system decrypts the data using a shared key. This allows information to transit the internet or the network without being captured and read by a threat actor monitoring the traffic.[58] The most visible example of encryption in transit is the Hyper Text Transfer Protocol Secure (HTTPS) used for visiting web sites.

Administrative controls can be a highly effective tool for protecting data. From an organizational perspective data governance is a necessity in reducing risk to the organization.

- Policy - Policies that define the appropriate use of applications and services provided by the organization are fundamental in helping to resolve human resource issues. If an employee is terminated for browsing pornographic websites at work a policy had better been in place prior to the termination or the organization may face a wrongful termination lawsuit. Most individuals would intrinsically understand inappropriate workplace behavior but if there are no rules written down and disseminated to staff, the terminated employee would likely win their wrongful termination suit.
- Contracting - Another administrative control that is highly useful is a contract review process that includes a review for provisions on information security and privacy. It is not enough to have a business associate agreement in place, an organization must define the lowest level of security they are willing to accept from a vendor or a partner to secure their data. This is a risk-based decision that the organization may need to make if the vendor is not willing to budge on contracting provisions.
  - o Ensure that the vendor addresses security and privacy controls within a contract. Information should be a shared responsibility, but many contracts place all responsibility for product security on the customer.
  - o If the vendor uses hosted solutions make sure there is language that covers these downstream services.
  - o If the language in the contract is weak, work with the legal team and the information security team in the organization to build template language for negotiating contracts.
  - o Be aware of the risks of "*click through agreements*." These are contract agreements for services that usually come in the form of a webpage when paying for a service online.[68] If "I agree" is clicked then all the terms and conditions have been agreed to by the organization. These are non-negotiable agreements and could place patient privacy or security at risk if they do not include protective language. They will certainly benefit the vendor and place all the risk on the customer. Employees of a healthcare entity should also be aware that they are accepting risk on behalf of the organization if they click these agreements. Organizations will likely have a signature authority policy in place

that identifies who in the organization can sign contracts.

Physical controls are very important in protecting the security and privacy of data and individuals who are part of the healthcare environment including employees, visitors, and patients. In addition to having guards, gates, cameras, and door locks there are other controls that protect the environment that are not so obvious.

- Proximity cards are used widely in healthcare to restrict access to certain areas. These cards are typically an ID badge worn by the employee and given rights to access areas where they can go. In addition to unlocking doors, proximity cards can be used to unlock workstations or cabinets.
- RFID (radio-frequency identification) uses electromagnetic fields to identify and track items.69 RFID tags can be attached to pieces of expensive mobile equipment like infusion pumps, wheelchairs, or beds to help locate these devices and deter theft. Additionally, these tags could be included in an armband for a newborn and hooked to a security system that automatically locks doors if there is an attempted abduction.
- Cameras can be used to monitor movement in the hallways or main areas of a hospital or clinic. They can also be used to monitor more sensitive areas like pharmacies. Additionally, cameras can be integrated into systems that help reduce fall risk. Some technologies draw virtual borders around beds or chairs and if the patient breaks that boundary it sends an alert to the main desk in the unit. This can be very effective in preventing falls from patients who are fall risks or in preventing a patient from eloping.

FUTURE TRENDS - EMERGING RISKS IN HEALTHCARE

Given the nature of the healthcare industry, it will continue to be viewed as a rich target for malicious actors. The provider segment of the industry within the United States operates in a manner which allows generous access to patients and visitors and relies on the free flow of information to safely provide care. This dynamic places data and computers at a higher-level risk for the theft of devices or data. The growth in the use of health technology only exacerbates this concern by increasing the attack surface and increasing the amount of sensitive data that could be infiltrated. However, this is not the limitation of emerging risks within healthcare.

Health technology not only stores and transmits sensitive information, it can be used to provide direct care to a patient. These technologies assist the nurses and doctors by automating certain tasks. Biomedical devices include many different types of technology that directly touch the patient; including infusion pumps that automatically deliver medications, ventilators which assist in breathing, surgical robots, and pacemakers. While these devices are extremely effective in assisting patients, they use computer code to ensure they function properly. Many of these devices may reside on an operating system similar to what is used on a desktop computer. When this is the case they have the same vulnerabilities that a desktop computer does, and they should also be patched and updated to reduce the risk of compromise.

Biomedical technology is typically managed by a clinical engineering department in a hospital. Traditionally the information technology department has not had a large role in managing these devices, so it is up to biomed to ensure that these devices are operating in a safe manner. This requires them to understand when and how the device should be patched or how the device should be secured on the network. More and more the biomed and IT departments are needing to cooperate to ensure these devices are appropriately secured.

There are several challenges to securing these devices. For one, these devices are reviewed and approved by the Food and Drug Administration (FDA) for use on patients. They go through a long application and review process before they are finally permitted for use. Biomedical device manufacturers want to ensure that the devices are operating as designed and so may be very proprietary about how they patch and support these devices. If a vendor has a restrictive support contract around these devices it can be challenging to receive timely updates. Vendors are allowed to patch these devices without going through the FDA approval process, as long as the security updates do not impact the functionality of the device. However, vendors may choose to bundle their patches and may take a considerable amount of time to test the patches to ensure there are no changes to functionality. The FDA has issued post market guidance on the cybersecurity of medical devices to help ease this process but there is a lot left in the hands of the manufacturer regarding security patching.[70]

Older devices can run on operating systems that are no longer supported by the vendor, thus compounding the issue. If a patch for a vulnerability is not available, the organization must evaluate different methods of securing the device.

The threat is very real. In May 2017 a virus named WannaCry impacted biomedical devices in the US and in Europe with ransomware that made the devices unusable for patient care.[71]

This virus also impacted environmental control systems. These too are an emerging avenue of compromise for hospitals and other care facilities. Environmental control systems manage the temperature and airflow within these buildings and are vital in keeping the appropriate temperature for care and maintaining proper airflow to reduce the risk of infection.

Environmental control systems, biomedical devices, and any other device connected to a healthcare network are going to increase the attack surface. The more vulnerable points on a network, the more chances an attacker must pivot and identify a higher profile target. If a biomedical device can be reprogrammed by an attacker, this device could be used to harm a patient. If an environmental control system can be hacked, and that system is shut down or reprogrammed, this too can have an impact on patient safety. This happened in Arlington, Texas in 2009 when an employee broke into 14 computers, installing malware that allowed others to control the computers. One of these computers controlled the heating and air conditioning for the hospital. The hacker was sentenced to nine years in federal prison for his crime.[72]

While patient privacy and the protection of sensitive information is very important, the ultimate risk lies in the potential physical harm that hacked systems could have on patients.

RECOMMENDED READING

Privacy and security are constantly evolving. There are new vulnerabilities, threats, breaches, and regulatory interpretations on a daily basis. To keep current on some of these issues please check out the following resources:

Wired magazine. https://www.wired.com/category/security/. In-depth security articles.

Krebs on Security. https://krebsonsecurity.com/. Security blog.

Ars Technica. https://arstechnica.com/. Technology news site.

The Register. https://www.theregister.co.uk/security/. International news site.

Health and Human Services. https://www.hhs.gov/hipaa/newsroom/index.html. HIPAA releases.

KEY POINTS

- Confidentiality, integrity and availability are key concepts to understand healthcare information privacy and security
- ARRA and the HITECH Act were designed in part to supplement the administrative, physical and technical safeguards implemented by HIPAA
- Healthcare workers must be able to identify different types of threat actors as well as the appropriate controls
- Security measures will continue to improve but so will the efforts of criminals who seek illicit access to protected health data and identify theft

CONCLUSIONS

This chapter has touched the surface of what it means to protect the privacy and security of health information. It has covered some basic concepts of information security, the healthcare privacy and security regulatory environment, business drivers and organizational structure of information security in healthcare, real healthcare breaches and consequences, threat actors, types of attacks, tools used to protect information, and some emerging security risks to the industry. This broad overview of privacy and security is just a primer to a segment of the healthcare industry that continues to evolve and mature.

Currently there is no way to predict what impacts the industry will face regarding security threats. Who would have predicted in January 2017 that National Security Agency cyber warfare tools would be leaked and then used with great impact against healthcare in the WannaCry attack of May 2017?[73]

To be effective in protecting privacy and security in healthcare it is important for all of those who work in the industry to be aware of the potential vectors of attack, type of information exposed, and the tools that can be used to prevent an attack. Ultimately, the information security and privacy practitioners of an organization rely on everyone in the workforce to be a partner in protecting our information assets and systems.

REFERENCES

1. Agaku IT, Adisa AO, Ayo-Yusuf OA, Connolly GN. Concern about security and privacy, and perceived control over collection and use of health information are related to withholding of health

information from healthcare providers. J Am Med Inform.2014;21(2):374-378

2. National Institute of Standards and Technology. FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION: Standards for Security Categorization of Federal Information and Information Systems. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf. Page 6. February 2004. (Accessed Sept 22, 2017)
3. National Institute of Standards and Technology. FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION: Standards for Security Categorization of Federal Information and Information Systems. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf. Page 2. February 2004. (Accessed Sept 22, 2017)
4. US-CERT, United States Computer Emergency Readiness Team. Defense in Depth. https://www.us-cert.gov/bsi/articles/knowledge/principles/defense-in-depth. September 13, 2005. (Accessed Sept 22, 2017)
5. U. S. Department of Health & Human Services. HIPAA Enforcement. https://www.hhs.gov/hipaa/for-professionals/special-topics/HITECH-act-enforcement-interim-final-rule/index.html. June 16, 2017. (Accessed Sept 22, 2017)
6. U. S. Department of Health & Human Services. HIPAA Enforcement. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html. July 25, 2017. (Accessed Sept 22, 2017)
7. U. S. Department of Health & Human Services. Guidance Materials for Consumers. https://www.healthit.gov/providers-professionals/implementation-resources/ocr-guidance-materials-consumers. N.D. (Accessed Sept 22, 2017)
8. U. S. Department of Health & Human Services. Covered Entities and Business Associates. https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html. June 16, 2017. (Accessed Sept 22, 2017)
9. U. S. Department of Health & Human Services. Won't the HIPAA Privacy Rule's minimum necessary restrictions impede the delivery of quality health care by preventing or hindering necessary exchanges of patient medical information among health care providers involved in treatment? https://www.hhs.gov/hipaa/for-professionals/faq/208/wont-minium-necessary-restriction-impede-delivery/index.html. March 14, 2006. (Accessed Sept 22, 2017)
10. Privacy Rights Clearinghouse. The HIPAA Privacy Rule: Patients' Rights. https://www.privacyrights.org/consumer-guides/hipaa-privacy-rule-patients-rights. September 23, 2017. (Accessed Sept 22, 2017)
11. U. S. Department of Health & Human Services. HIPAA Administrative Simplification. pg 16. https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf. March 26, 2013. (Accessed Sept 22, 2017)
12. U. S. Department of Health & Human Services. HIPAA Administrative Simplification. pg 84. https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf. March 26, 2013. (Accessed Sept 22, 2017)
13. U. S. Department of Health & Human Services. HIPAA Administrative Simplification. pg 78. https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf. March 26, 2013. (Accessed Sept 22, 2017)
14. U. S. Department of Health & Human Services. HIPAA Administrative Simplification. § 164.502 pg 77-80. https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf. March 26, 2013. (Accessed Sept 22, 2017)
15. U.S. Department of Health and Human Services National Institutes of Health. How can covered entities use and disclose protected health information for research and comply with the Privacy Rule. http://privacyruleandresearch.nih.gov/pr_08.asp. February 7, 2007. (Accessed Sept 22, 2017)
16. U. S. Department of Health & Human Services. Business Associates. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html. July 26, 2013. (Accessed Sept 22, 2017)
17. U. S. Department of Health & Human Services. Business Associate Contracts. https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html. June 16, 2017. (Accessed Sept 22, 2017)
18. U. S. Department of Health & Human Services. HIPAA Administrative Simplification. pg 63. https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf. March 26, 2013. (Accessed Sept 22, 2017)
19. U. S. Department of Health & Human Services. HIPAA Administrative Simplification. pg 64-66. https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf. March 26, 2013. (Accessed Sept 22, 2017)
20. U. S. Department of Health & Human Services. HIPAA Administrative Simplification. pg 71. https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf. March 26, 2013. (Accessed Sept 22, 2017)
21. U. S. Department of Health & Human Services. HIPAA Administrative Simplification. pg 71. https://www.hhs.gov/sites/default/files/

hipaa-simplification-201303.pdf. March 26, 2013. (Accessed Sept 22, 2017)

22. U. S. Department of Health & Human Services. HIPAA Administrative Simplification. pg 71. https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf. March 26, 2013. (Accessed Sept 22, 2017)
23. U. S. Department of Health & Human Services. HIPAA Administrative Simplification. pg 71-72. https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf. March 26, 2013. (Accessed Sept 22, 2017)
24. U. S. Department of Health & Human Services. HIPAA Administrative Simplification. pg 72-73. https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf. March 26, 2013. (Accessed Sept 22, 2017)
25. U. S. Department of Health & Human Services. Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf. N.D. (Accessed Sept 22, 2017)
26. U.S. Department of Health and Human Services. Office for Civil Rights. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html. May 23, 2017. (Accessed Sept 22, 2017)
27. Finkle, J. and Burns, D. St. Jude stock shorted on heard device hacking fears; shares drop. http://www.reuters.com/article/us-stjude-cyber/st-jude-stock-shorted-on-heart-device-hacking-fears-shares-drop-idUSKCN1101YV. August 25, 2016. (Accessed Sept 22, 2017)
28. Beazley. Beazley Breach Response (BBR) in Technology, media & business services: Healthcare. https://www.beazley.com/documents/Factsheets/beazley-bbr-coverage-factsheet-us.pdf. N.D. (Accessed Sept 22, 2017)
29. McCann E. Behemoth breach sounds alarm for 4M. http://www.healthcareitnews.com/news/behemoth-hipaa-breach-sounds-alarms. August 26, 2013. (Accessed Sept 22, 2017)
30. McCann E. Advocate health slapped with lawsuit after massive data breach. http://www.healthcareitnews.com/news/AdvocateHealth-slapped-with-lawsuit-after-massive-data-breach. September 6, 2013. (Accessed Sept 22, 2017)
31. Conn J. Advocate health care sued following massive data breach. http://www.modernhealthcare.com/article/20130906/NEWS/309069953. September 6, 2013. (Accessed Sept 22, 2017)
32. Ouellette, P. Oregon Health and Science University reports data breach. https://healthitsecurity.com/news/oregon-health-and-science-university-reports-data-breach. March 26, 2013. (Accessed Sept 22, 2017)
33. Ouellette, P. OHSU alerts patients of Google cloud security concerns. https://healthitsecurity.com/news/ohsu-alerts-patients-of-google-cloud-security-concerns. July 29, 2013. (Accessed Sept 22, 2017)
34. U.S. Department of Health and Human Services. Office for Civil Rights. Widespread HIPAA vulnerabilities result in $2.7 million settlement with Oregon Health & Science University. http://wayback.archive-it.org/3926/20170127185938/https://www.hhs.gov/about/news/2016/07/18/widespread-hipaa-vulnerabilities-result-in-settlement-with-oregon-health-science-university.html. July 18, 2016. (Accessed Sept 22, 2017)
35. U.S. Department of Health & Human Services. Breaches affecting 500 or more individuals. https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html. Updated July 26, 2013. (Accessed Sept 22, 2017)
36. Privacy Rights Clearinghouse. Data breaches: a year in review. https://www.privacyrights.org/blog/data-breaches-year-review. December 16, 2011. (Accessed Sept 22, 2017)
37. Vockley M. Safe and secure? Healthcare in the Cyberworld. Biomedical Instrumentation & Technology. 2012; 164-173 https://doi.org/10.2345/0899-8205-46.3.164. (Accessed Nov 25, 2013)
38. Kern, C. Judge Tosses Most Claims in DoD, TRICARE Data Breach Case. https://www.healthitoutcomes.com/doc/judge-tosses-most-claims-in-dod-tricare-data-breach-case-0001. May 16, 2014. (Accessed Sept 22, 2017)
39. Conn J. HHS wants photocopy machines examined as part of data security. http://www.modernhealthcare.com/article/20130815/NEWS/308159953. August 15, 2013. (Accessed Sept 22, 2017)
40. Office of Civil Rights. HHS settles with health plan in photocopier breach case. http://wayback.archive-it.org/3926/20170127183806/https://www.hhs.gov/about/news/2013/08/14/hhs-settles-with-health-plan-in-photocopier-breach-case.html. August 14, 2013. (Accessed Sept 22, 2017)
41. Giandomenico, A. Byline: Know Your Enemy: Understanding Threat Actors. https://blog.fortinet.com/2017/07/13/byline-know-your-enemy-understanding-threat-actors. July 13, 2017. (Accessed Sept 22, 2017)
42. Recorded Future. Proactive Defense: Understanding the 4 Main Threat Actor Types. https://www.recordedfuture.com/threat-actor-types/. August 23, 2016. (Accessed Sept 22, 2017)
43. Zetter, K. That Insane, $81M Bangladesh Bank Heist? Here's What We Know. https://www.wired.com/2016/05/

insane-81m-bangladesh-bank-heist-heres-know/. May 17, 2016. (Accessed Sept 22, 2017)

44. Australian Competition & Consumer Commission. Nigerian Scams. https://www.scamwatch.gov.au/types-of-scams/unexpected-money/nigerian-scams. N.D. (Accessed Sept 22, 2017)
45. Walls, M. Nation-State Cyberthreats: Why They Hack. https://www.darkreading.com/informationweek-home/nation-state-cyberthreats-why-they-hack-/a/d-id/1318522?. January 8, 2015. (Accessed Sept 22, 2017)
46. Barreiro, A. Defending against Advanced Persistent Threats. http://www.techrepublic.com/blog/it-security/defending-against-advanced-persistent-threats/. April 16, 2012. (Accessed Sept 22, 2017)
47. Peterson, A. The Sony Pictures Hack, Explained. https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?utm_term=.a9563cad386d. December 18, 2014. (Accessed Sept 22, 2017)
48. Greenberg, A. How an Entire Nation Became Russia's Test Lab for Cyberwar. https://www.wired.com/story/russian-hackers-attack-ukraine/. June 20, 2017. (Accessed Sept 22, 2017)
49. Harwell, D. and Nakashima, E. China Suspected in Major Hacking of Health Insurer. https://www.washingtonpost.com/business/economy/investigators-suspect-china-may-be-responsible-for-hack-of-anthem/2015/02/05/25fbb36e-ad56-11e4-9c91-e9d2f9fde644_story.html?utm_term=.80c71d4081ab. February 5, 2015. (Accessed Sept 22, 2017)
50. Lord, M. What is Social Engineering? Defining and Avoiding Common Social Engineering Threats. https://digitalguardian.com/blog/what-social-engineering-defining-and-avoiding-common-social-engineering-threats. July 27, 2017. (Accessed Sept 22, 2017)
51. Phishing.org. What is Phishing? http://www.phishing.org/what-is-phishing. N.D. (Accessed Sept 22, 2017)
52. Armasu, L. Spreading Malware Through Dropped USB Sticks Could Be Highly Effective Research Finds. http://www.tomshardware.com/news/dropped-usb-sticks-spreads-malware,32391.html. August 4, 2016. (Accessed Sept 22, 2017)
53. US-CERT, United States Computer Emergency Readiness Team. Security Tip (ST04-015) Understanding Denial-of-Service Attack. https://www.us-cert.gov/ncas/tips/ST04-015. February 6, 2013. (Accessed Sept 22, 2017)
54. Hilton, S. Dyn Analysis Summary of Friday October 21 Attack. https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/. October 26, 2016. (Accessed Sept 22, 2017)
55. University of Virginia Computer Science. Blocking Brute Force Attacks. http://www.cs.virginia.edu/~csadmin/gen_support/brute_force.php. 2007. (Accessed Sept 22, 2017)
56. C.S-W. The Economist. What doxxing is, and why it matters. https://www.economist.com/blogs/economist-explains/2014/03/economist-explains-9. March 10, 2014. (Accessed Sept 22, 2017)
57. Johnson, B. What is Next-Generation Antivirus (NGAV)? https://www.carbonblack.com/2016/11/10/next-generation-antivirus-ngav/. November 10, 2016. (Accessed Sept 22, 2017)
58. Raglione, A. Best Practices: Securing Data at Rest, in Use, and in Motion. https://www.datamotion.com/2015/12/best-practices-securing-data-at-rest-in-use-and-in-motion/. December 1, 2015. (Accessed Sept 22, 2017)
59. Harris S, Ouellet E. Security+ Certification All-in-One Exam Guide. Berkeley, CA:McGraw-Hill/Osborne; 2003.
60. Ismail, N. Access all areas? Tracking and managing the privileged users. http://www.information-age.com/access-areas-tracking-managing-privileged-users-123465270/. March 27, 2017. (Accessed Sept 22, 2017)
61. OWASP. Welcome to OWASP the free and open software security community. https://www.owasp.org/index.php/Main_Page. March 13, 2017. (Accessed Sept 22, 2017)
62. OWASP. OWASP Top 10 Proactive Controls 2016. https://www.owasp.org/index.php/OWASP_Proactive_Controls. September 1, 2017. (Accessed Sept 22, 2017)
63. Secureworks. Vulnerability Assessments Versus Penetration Tests. https://www.secureworks.com/blog/vulnerability-assessments-versus-penetration-tests. April 8, 2015. (Accessed Sept 22, 2017)
64. Palo Alto Networks. What is a Firewall? Firewalls and Their Evolution. https://www.paloaltonetworks.com/cyberpedia/what-is-a-firewall. N.D. (Accessed Sept 22, 2017)
65. SANS Institute InfoSec Reading Room. Understanding Intrusion Detection Systems. https://www.sans.org/reading-room/whitepapers/detection/understanding-intrusion-detection-systems-337. 2001. (Accessed Sept 22, 2017)
66. Kaspersky Lab. What is a Web Filter? https://usa.kaspersky.com/resource-center/definitions/web-filter. 2017. (Accessed Sept 22, 2017)
67. Cisco. Chapter: Understanding and Configuring VLANs. https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/vlans.html. N.D. (Accessed Sept 22, 2017)
68. Wilmer Hale. Are "Click Through" Agreements Enforceable? https://www.wilmerhale.

com/pages/publicationsandNewsDetail.aspx?NewsPubId=86850. March 22, 2000. (Accessed Sept 22, 2017)

69. PC Mag. Definition of: RFID. https://www.pcmag.com/encyclopedia/term/50512/rfid. N.D. (Accessed Sept 22, 2017)

70. U.S. Food and Drug Administration. Cybersecurity. https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm. August 30, 2017. (Accessed Sept 22, 2017)

71. Fox-Brewster, T. Medical Devices Hit By Ransomware For The First Time In US Hospitals. https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/#19a26c9a425c. May 17, 2017. (Accessed Sept 22, 2017)

72. Moscaritolo, A. Texas hospital hacker sentenced to nine years. https://www.scmagazine.com/texas-hospital-hacker-sentenced-to-nine-years/article/558753/. March 21, 2011. (Accessed Sept 22, 2017)

73. Nakashima E. The NSA has linked the WannaCry computer worm to North Korea. https://www.washingtonpost.com/world/national-security/the-nsa-has-linked-the-wannacry-computer-worm-to-north-korea/2017/06/14/101395a2-508e-11e7-be25-3a519335381c_story.html?utm_term=.1d32be0c6a5d. June 14, 2017. (Accessed Sept 22, 2017)