An Evaluation of the Cybersecurity Policies for the United States Health & Human Services Department

Derek Mohammed PhD[1], Ronda Mariani[2]

ARTICLE INFO

Available Online April 2014
Key words:
Cybersecurity Policy;
Health Department;
Evaluation;
Regulation;
Recommendation.

ABSTRACT

This paper examines the criteria necessary for the evaluation of the cybersecurity policies for the United States Health and Human Services Department of the Federal Government. The overall purpose of cybersecurity policies and procedures is supported through compliance with Federal mandated regulation and standards, which serve to protect the organizational services and goals of the United States Health and Human Services Department, and to promote the best possible security practices in the protection of information systems from unauthorized actors and cyber-threats. The criteria of the cybersecurity evaluation is identified and analyzed for quality, strengths, weaknesses, and future applicability. Topics within the criteria include organizational operation, regulations and industrial standards compliance, service delivery to national customers, and the prevention and mitigation of IT system and security failure. This analysis determines the strengths and weaknesses, and makes recommendations for revising the cybersecurity policies within the United States Health and Human Services Department.

1. Introduction

The cybersecurity policy framework for the United States Health and Human Services Department (Health Department) requires periodic revisions and additions to ensure proper policy standards and procedures are effective in deterring cyber-threats, and satisfying Federal regulatory compliance. Just as technology becomes outdated; policies lose relevance and effectiveness with the arrival of new service offerings and improved digital processes. As a Federal entity and a critical infrastructure sector, the Health Department manages national health care, food, pharmaceuticals, and public health services (Government Accountability Office, [GAO], 2010). The Health Department maintains the flagship identity for both public and private entities within the healthcare sector, which requires departmental security practices to be exceptional in order to provide a model for Federal subdivisions of the Health Department. National cybersecurity coordinators within the Federal Government task the Federal departments and agencies with promoting security through partnerships with both public and private stakeholders, and according to a survey of fifty-six private sector entities in 2010, estimated requests for information sharing and threat alerts were met only one-third of the time (GAO, 2010). This statistic is lackluster, and demonstrates the importance of increasing the cybersecurity environment within the Federal Government, and the Health Department maintains an information security policy lifecycle.

The Health Department consists of many operating divisions and sub divisions, which are all subject to the department level information technology (IT) and security umbrella policies, in addition to their respective policy frameworks. As a public sector entity, the Health Department appoints the Chief Information Security Officer and Deputy Security Officers. These political appointments result in a change of personnel periodically which disrupts operational continuity. As a result of these changes there are different priorities which ultimately affects the enterprise security framework. Due to this dilemma, policy must meet standardized criteria, which can be maintained with minimal revisions through an IT and personnel refresh cycle (Biddick, 2009). Federal IT teams and policy stakeholders are currently prioritizing information security, as both internal and external cyber-threats have become public knowledge, and directly threaten the operation and service delivery of the Health Department. Within this prioritization, strategies for

[1] Associate Professor of Computer Information Systems, Department, School of Business, Saint Leo University, United States, Email: derekmohammed@yahoo.com
[2] Assistant Professor of Management, Department, School of Business, Saint Leo University, United States Email: Ronda.mariani@saintleo.edu

database consolidation, and the new classification of big data, must be addressed by the Health Department (Biddick, 2011). In order to promote proper compliance with the cybersecurity procedures and standards established by the Department, the current cybersecurity policy framework must be analyzed to verify that critical success factors are being met, and the criteria for the best-possible cybersecurity and information assurance aspects are evaluated for quality, strengths, weaknesses, and future applicability.

The primary goal of the Health Department is to comply with Federal regulations relating to the protection of sensitive information. According to the National Institute of Standards and Technology (NIST), the Health Department is obligated to classify, protect, and discreetly handle sensitive information categorized as personally identifiable information (PII). Furthermore, the context in which PII is handled by the Health Department's workforce must be detailed in the cybersecurity policy (McCallister, Grance, & Scarfone, 2010). PII, defined as unique information, which can distinguish, trace, or link information to an individual or identity, is prevalent in the delivery and management of services provided by the Health Department. Since the Health Department is a Federal entity, the customer base is nation-wide.

The handling of big data requires further classification of data. The United States Department of Health and Human Services(2003) issued the Standards for Privacy of Individually Identifiable Health Information as a privacy rule in the implementation of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), to provide guidance in the classification of data. This was done in order to streamline data handling processes and prevent improper allocation of security resources. This rule reclassified Department-specific data as Protected Health Information (PHI), which is defined as an individual's past, present, or future physical or mental condition, a health care provision, or any healthcare related payment information. In prioritizing the protection of potential cybersecurity targets, the Office of the Chief Information Officer within the Health Department establishes policy to protect PII and PHI by establishing information assurance policies, and best-practice policies for accessing all platforms of the overall information system.

2. Literature Review

According to Whitman and Mattord (2014), a cybersecurity policy uses an organization's vision and mission to align and customize its security planning, issues, risk assessment, program implementation, monitoring, and evaluation. In addition, it outlines the roles of cybersecurity and management personnel in the execution of these processes. In essence, it also indicates the commitment of the organization and its leaders to deploy resources and training where necessary to ensure a secure environment for operational and stakeholder purposes. A policy, once written, acts as a living document and has to change as technology advances. Similarly, Hone and Eloff (2002) also stated that a security policy should be living document, which must be updated on a regular basis. In fact, Knapp, Morris, Marshall and Byrd (2009) comment that a policy should also evolve depending on changes in operational decisions and outcomes that the organization makes. Further, the need to amend a cyber-security policy also depends on the legal and regulatory context in which it operates, as such, it will vary by industry and region.

In 2006, Siponen and Iivaris stated that cybersecurity policies require more frequent reviews than any other company policy. More specifically, the contents of a comprehensive cybersecurity policy should address the roles and responsibilities of users, define the boundaries of authorized and unauthorized system usage, and penalties for its violation. Additionally, it should also include a mechanism for reporting and dealing with security threats to the system. Such an approach ensures that once it is operationalized and updated as the context changes, a cybersecurity policy will become integrated into the management of an organization and affect its communication and decision making norms used by the entire body of employees and administrators alike(Whitman & Mattord, 2014).

While this seems to be a logical and simple approach, there are numerous types of industries, corporations, governmental and non-governmental agencies that exist each with its specific operational and security needs. To match this, numerous policy models have evolved with an ever-expanding body of literature. According to Doherty, Anastasakis and Fulford (2009)there appears to be an imbalance in the body of literature dealing with the structure of cybersecurity models and paucity of empirical evidence and consensus. As more measures are taken towards standardization in the field such an imbalance will be redressed. Moving from the general to the specific, is what follows in an evaluation of the criteria used by a specific governmental agency in its cybersecurity policy.

3. Overview of Evaluation Criteria

The cybersecurity policies and technical controls present in the security framework of the Health Department must be specific to the information systems and the variables present in the cyberspace environment, which may threaten or cause destruction to overall organizational operation. By establishing common criteria for the basis, analysis, and evaluation of all information assurance and cybersecurity policies, the resulting operational consistency in policy requirements can generate effective cybersecurity policies across the Health Department operating divisions. Common criteria must account for both technical controls and the human element of cybersecurity compliance. In additional to common criteria for policy evaluation, NIST recommends that Government departments establish performance measures for the evaluation of cybersecurity policies, and for the implementation of selected security controls necessary to the information systems (Radack, 2008). Performance measures serve as metrics for policy officers within the Health Department, and allow reporting on both technical and policy security aspects. These measures are used to make future recommendations for policy changes.

3.1 Common Criteria

In this evaluation, the common criteria for the Health Department cybersecurity policies consists of eight attributes, which affect the stability and presence of the information security operations. These attributes are: authority, action-ability, accuracy, appropriateness, exceptions relevance, specificity, and violations. Each of these attributes applies to different levels of security personnel and operations. From the perspective of risk management, combining a broad security philosophy with technical specification enables security efforts to be unconstrained by technical and procedural complexity. Complexity in policy compliance can generate workforce resistance, internal conflicts, and overall dissatisfaction with IT and cybersecurity security measures (Kefallinos, Lambrou,& Sykas, 2009). Another form of criteria, which is cross referenced through the evaluation process, and used to forecast future policy recommendations and changes, is S.M.A.R.T (SMART). SMART stands for specific, measurable, attainable, relevant, and time bound and it is a set of baseline principles used as guidance for setting goals. The key to identifying a successful policy is to understand its realistic application in a specific work environment.

Realistic application of cybersecurity policies within the Health Department rely on the assessment of qualitative and quantitative risks. Both of these factors are important in the assessment and evaluation of security policies, because they account for different measurable aspects. Qualitative risks involve conflicts, inconsistencies, and vulnerabilities, which are identified through the analysis of non-numerical data and observation. This primarily includes, but is not limited to, poor security practices, lack of compliance in audits for Federal regulation, and an overall weak information security definition and presence. Because the Health Department delivers services to the public health sector, qualitative risks also can potentially damage the organization's ability to serve the public and other Federal agencies and departments. Today's cyber-threats possess the ability to cross the logical cyberspace plane to physical reality.This is done via attacks on critical infrastructure and industrial control systems, such as Supervisory Control and Data Acquisition systems (SCADA). The existence of these new cyber-threats promotes the necessity for cybersecurity policy to emphasize the protection and maintenance of information and IT availability, which can adversely affect the entire operation of the Health Department, if not properly secured (GAO, 2010).

Quantitative risks are primarily, but not limited to, the numerical cause of risk exploitation. For example, if the handling of sensitive information has been identified as a qualitative risk, auditors and policy stakeholders can investigate the statistical evidence and percentages of incidents of where and how information may have been compromised and leaked. However, this can only occur if a proper policy covering this aspect isinitially in place. Quantitative risk assessments can also provide historical data and evidence to support or criticize both policy and technical security controls(Gibson, 2011). Because of this, a risk assessment must be an important tool in evaluating a policy, and the inclusion of risk metrics in an evaluation can assist in the analysis of poorly defined security practices, which may not be directly observable and measureable.

According to Gibson (2011), although a qualitative risk can be generated and come from the human element threat spectrum, a quantitative risk can both cause and be the cause of a qualitative risk. Furthermore, a failure in technical security controls, such as the access control system, can compromise proper authentication within an information system, and put both databases and overall system operations at risk. Within the Health Department, the PHI and PII of the national population is managed in large databases.This

exposes it to both quantitative and qualitative risks. The organizational image and reputation of the Department can be impacted with a reported information breach, which also causes financial impacts through the replacement, reimbursement, or damage remediation of lost and compromised records. Within the policy spectrum, the Health Department must account for uncertainties in policy controls and implementation. These uncertainties are essential risks, and incidents resulting from risk exploitation, must be anticipated and planned for.

3.2 Federal Regulation and Standards

In the evaluation of cybersecurity policies, the Health Department is classified as an entity of the Federal Government and an organization with a national customer base. Price Waterhouse Cooper (PwC), a private liability and risk management firm, is contracted by the Health Department to conduct risk assessments for the department and the operating divisions' privacy policies and incident reporting. According to a research report by PwC's Health Research Institute in 2011, the health industry is not fully prepared to protect the privacy of its customers, as two-thirds of the breaches involved the theft of PII and PHI. The risks arose from a lack of mobile device policies, and improper handling of sensitive information by internal staff. PwC also notes that a majority of breaches within the health industry originate from internal cyber-threats and insider data leakage, as opposed to external cyber-threat actors, such as hackers (Milliard, 2011). This report emphasizes the necessity for the cybersecurity policies of the Health Department to be able to accommodate new technology (e.g. mobile devices), and to be relevant in dictating proper guidance and standards in the definition and handling of sensitive information.

The Federal Government recognizes the need to protect sensitive information pertaining to Health IT, and has enacted Federal regulation, paired with information security guidance, to ensure the Health Department, as well as other Federal Departments, have consistent resources and strategies in developing cybersecurity policy frameworks. The two primary regulations which the Health Department must comply with are HIPAA, and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH). HIPAA, which defines PII and PHI as sensitive information, was implemented in 1996, because of the influx in technology systems being utilized to store electronic health records. According to NIST, HIPAA defines a security rule, which protects the confidentiality, integrity, and availability of PHI covering the following entities: healthcare providers who utilize electronic record keeping, health insurers, healthcare clearinghouses, and prescription drug card sponsors. Furthermore, HIPAA requires both physical and technical security safeguards in the protection of PHI (Scholl et al., 2008). These required safeguards influence the overall cybersecurity and physical security frameworks of the Health Department. This regulation factors into the categorization of information systems and the separation of duties within the workforce via access control systems to ensure that only authorized personnel with proper training in the handling of sensitive information have access.

The HITECH Act serves as an update for HIPAA, because it recognizes that technology must be appropriate in order to successfully promote security of electronic records and sensitive information. Privacy of information, which is a concern of cybersecurity, is the legal right of the healthcare sector customer. The concern arises where information can be easily accessed, modified, or deleted if the proper safeguards are not present. Since a breach in PII and PHI can result in the Health Department having a failure in service or potentially taking a financial loss, the HITECH Act requires privacy incident reporting and incident response planning for breaches involving over 500 records (Grant Thornton Ltd, 2013). The legal consequences for non-compliance in incident reporting are strict, with a maximum penalty of $1.5 million for all violations, and four tiers of infractions, which have individual monetary penalties. These penalties can be enforced on both private entities and the Health Department operating divisions. Because HITECH offers no waiver system or affirmative defense for absent incident reports, failure to make a diligent effort to report breaches can result in further civil penalties, and a $50,000 minimum fine per penalty (Grama, 2011). In order to comply with HIPAA and the HITECH Act, best practices and policy guidelines are provided by the National Institute of Standards and Technology, which publishes and revises special publications based on aspects of information security. These aspects are based on the requirements set forth in the Federal Information Security Management Act of 2002 (FISMA), and are consistent throughout the Federal Government IT realm.

4. Policy Evaluation

The following section will review and evaluate the Health Department Information Systems Security and Privacy Policy Framework, which serves as the overarching cybersecurity policy. In 2012, the Health Department introduced policy addendums for newly implemented technology, such as mobile devices and onsite wireless connectivity (Wi-Fi) for both Federal and privately contracted employees. While these additions are notable, the Health Department needs more security accommodations and controls in order to maintain relevant content within both the overarching policy and policy addendums.

4.1 Strengths and Weaknesses

The strengths and weaknesses of the Health DepartmentPolicy for Information System Security and Privacy (available from the Department website) are evaluated using the eight attributes of common criteria. Table 1 illustrates the evaluation of the policy criteria.

Table 1 Evaluation of Policy Criteria

Common Criteria Aspect	Strengths	Weaknesses
Accuracy The clarity of language and how it applies to the corresponding IT environment.	The policy presents all department-wide program controls for both technical and policy controls. All controls are referenced with policy addendums and the associated NIST guidance documents.	The policy addendums are not directly attached to the overarching policy; and therefore are subject to revision prior to the overarching policy revisions. This can create inconsistencies.
Action-ability The ability to implement the policy into action.	The policy details broad security controls, which allow better implementation for scaling operating divisions within the department.	The lack of detailed guidance and the overwhelming responsibility of the Office of the Chief Information Officer (OCIO) to assist operating divisions in implementation lowers the action-ability rating.
Appropriateness The suitability of the policy within the corresponding environment.	All security controls presented in the policy are present in NIST to be set in compliance with the minimum standards of FISMA.	N/A
Authority The identification and support of leadership, management, and enforcement.	The policy is mandated by the OCIO and explains the roles and responsibility of each departmental security officer. The user and technology services are clearly defined.	N/A
Exceptions The waiver process, which provides concessions and/or exemptions from policy.	The policy states that the OCIO has the authority to place a waiver on security controls on a case-by-case basis.	Currently, the leadership within the OCIO will not approve a waiver unless the security control is an impediment on organizational operation. There is no policy present for waiving personally owned technology devices.
Relevance The significance and applicability of the policy within the IT environment.	The policy includes aspects of information assurance, such as privacy impact assessments, media protection and sanitization, and a thorough awareness and training program. All aspects of health sector IT security are clearly defined.	N/A Note: As NIST releases updated guidance on the protection and encryption of PII and PHI, the overarching policy will be updated to include more health sector themed IT strategies.

Specificity The level of detail presented in the policy.	All security controls are divided by section in accordance with NIST guidance, and include policy action statements. These action statements include the requirement, parties involved, and the statement for rationale.	The statements for rationale have proper citations to Federal regulation, but include technical jargon, which may not be understood by non-technical parties.
Violations The consequences present for policy violations and non-compliance.	N/A	Impact levels and the measures taken against parties who do not fall into compliance are briefly mentioned; however, a violations clause is not present within the overarching policy.

Based on the analysis of the overarching cybersecurity policy, there are aspects of the common criteria, which prove that the policy needs further revision to ensure proper security presence and compliance. While all policies are subject to constant review and criticism, the action-ability, exceptions and violation of the Health Department overarching policy must be a focal point of the next revision. The action-ability of a policy is important in implementing and enforcing the policy statements. Exceptions to the policy are minimal, which is advantageous from a security point of view, but may hinder operation and overall workforce satisfaction with the policy. In conjunction with action-ability, the Health Department has put forward lenient violation penalties for non-compliance, which are not centralized in the policy itself. Allowing the OCIO to make judgment calls for security concerns can result in inconsistencies in security operations and inaccurate asset management across the operating systems of the department.

In concluding the evaluation of the overarching cybersecurity policy for the Health Department, the author has analyzed the previously established common criteria and identified strengths and weaknesses which can be revised and improved. The authority of the OCIO must assume a stronger, more authoritarian role in the enforcement of department-wide policies. Rules of behavior and guidelines for personal use of IT assets must be outlined in the primary policy, and addendums must be installed to the overarching policy to accommodate a waiver process for personally owned devices, such as smart phones. A policy helpdesk must also be established to clarify all questions regarding both policies and addendums, and provide guidance for both technical and non-technical personnel. Unacceptable use of IT assets must also be outlined and agreed to in writing by all personnel. Violations for non-compliance in all policies must be the cornerstone of the overarching cybersecurity policy. Further, the authority held by within the OCIO and Health Department must be used to inflict unbiased penalties where necessary. Performance measures, such as internal audits and vulnerability assessments must also occur periodically, prior to a scheduled policy revision meeting.

5. Conclusion

This paper provides the Health Department with the necessary points of focus to be utilized in future reevaluations of all applicable cybersecurity policies. The common criteria and pertinent Federal Government regulations must be consulted and used as a basis in applying new technical and physical security aspects to the overall cybersecurity framework of the Health Department. The current and future cyber-threat environment is increasing in hostility and widening in the diversity of threats. As a flagship organization of the public health sector for the United States, the Health Department is responsible for providing and following the best practices for successful information assurance.

References

Biddick, M. (2009). *InformationWeek Analytics: Government IT Priorities*. InformationWeek. Retrieved from http://www.informationweek.com/government/enterprise-architecture/informationweek-analytics-government-it/218500752

Biddick, M. (2011). *Research: Federal Government's IT Priorities*. InformationWeek. Retrieved from http://www.informationweek.com/government/leadership/research-federal-governments-it prioriti/231700118

Doherty, N. F., Anastasakis, L.,&Fulford, H. (2009). The information security policy unpacked: A critical study of the content of university policies. *International Journal of Information Management, 29*(6), 449-457.

Gibson, D. (2011). *Managing Risk in Information Systems*. Burlington, MA: Jones and Bartlett Learning.

Government Accountability Office. (2010). *Critical Infrastructure Protection Key Private and Public Cyber Expectations Need to Be Consistently Addressed*(GAO Publication No. 10-628). Retrieved from http://www.gao.gov/assets/310/307222.pdf

Grama, J. L. (2011). *Legal Issues in Information Security.* Burlington, MA: Jones and Bartlett Learning.

Grant Thornton Ltd. (2013). *HIPAA/HITECH Cybersecurity Solutions Advisory Services*. Retrieved from http://www.gt.com/staticfiles/GTCom/Advisory/IT/HIPAA%20HITECH%20Cybersecurity%20solutions/Grant%20Thornton%20HIPPA-HITECH%20Solutions.pdf

Hone, K., &Eloff, J.P. (2002). What makes an effective information security policy?*Network Security*, 6(1), 14-16.

Kefallinos, D., Lambrou, M.A., &Sykas, E. D. (2009). An Extended Risk Assessment Model for Secure E-Government Projects. *International Journal of Electronic Government Reserach,* 5, 72-92.

Knapp, J., Morris, F., Marshall, T., & Byrd, T. (2009). Information security policy: An organizational-level process model. *Computers and Security, 28*(7), 493-508.

McCallister, E., Grance, T., & Scarfone, T. (2010). *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* (NIST Special Publication 800-122). Retrieved from http:// csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

Milliard, M. (2011). *PwC: Health Industry Under-Prepared to Protect Privacy*. Retrieved from http:// www.healthcarefinancenews.com/news/pwc-health-industry-under-prepared-protect-privacy

Radack, S. (2008). *Using Performance Measurements to Evaluate and Strengthen Information System Security.* Retrieved from http://csrc.nist.gov/publications/nistbul/Sept-2008-bulletin.pdf.

Scholl, M., Stine, K., Hash, J., Bowen, P., Johnson, A., Smith, C. D., & Steinberg, D. I. (2008). *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.* Retrieved from http://csrc.nist.gov/ publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf

Siponen, M., &Iivari, J.(2006). Six Design Theories for IS Security Policies and Guidelines. *Journal of the Association for Information Systems, 7(7)*, 445- 472.

U.S. Department of Health and Human Services, Office for Civil Rights. (2003). *Summary of the HIPAA Privacy Rule.* Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/ privacysummary.pdf

Whitman, M. E., & Mattord, H. J. (2014). *Management of Information Security*. Boston, MA: Course Technology.