2018

A Multi-Objective Framework for Information Security Public Policy: The Case of Health Informatics

Kane Smith
Virginia Commonwealth University

A Multi-Objective Framework for Information Security Public Policy: The Case of Health Informatics

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy at Virginia Commonwealth University.

By

Kane J. Smith, PhD. Candidate
Virginia Commonwealth University,
Dept. Of Information Systems

Committee Members:

Dr. Lemuria Carter, Chair, VCU Department of Information Systems
Dr. Gurpreet Dhillon, Co-Chair, UNCG Department of Information Systems
Dr. Peter Aiken, VCU Department of Information Systems
Dr. Manoj Thomas, VCU Department of Information Systems
Dr. Jason Merrick, VCU Department of SCMA

Virginia Commonwealth University
Richmond, Virginia

April, 2018

Chapter Structure:

List of Tables

List of Figures

Abstract

TITLE: A MULTI-OBJECTIVE FRAMEWORK FOR INFORMATION SECURITY PUBLIC POLICY: THE CASE OF HEALTH INFORMATICS

By Kane J. Smith, Ph.D.

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy at Virginia Commonwealth University.

Virginia Commonwealth University, 2018.

Dissertation Director: Lemuria Carter, Ph.D., Department of Information Systems

Detailed holistic patient data is critical for healthcare organizations to better serve their patient populations. This information allows healthcare organizations to create a detailed and holistic record of a patient's health. However, this large aggregation of personally identifiable patient data raises serious privacy and security concerns amongst patients. For this reason, patient concerns around the privacy and security of information retained by healthcare organizations must be addressed through the development of effective public policy. This research, therefore argues that any decision making process aimed at developing public policy dealing with patient data privacy and security concerns should not only address regulatory concerns, but also patient-centric values. To accomplish this task, multi-objective decision analytic techniques, with Nissenbaum's (2004) contextual integrity as a normative framework are used. This is done to elicit patient-centric preferences to assist organizations and governmental institutions alike in dealing with their privacy and security concerns around patient data stored by Healthcare Systems.

Introduction

Detailed holistic patient data is critical for healthcare organizations to better serve their patient populations. By storing data related to patients in an Information System, it provides healthcare organizations and their physicians numerous benefits with respect to enhancing patient care and improving both clinical and organizational outcomes (King et al. 2014; Patel et al. 2015). When healthcare organizations record this data in the form of a patient record, it can contain two types of patient information (Fundamentals of the Legal Health Record and Designated Record Set n.d.): One, the legal medical record of patient health information, also known as an Electronic Medical Record (EMR), which is the documentation of healthcare services provided to an individual during any aspect of healthcare delivery in any type of healthcare organization and Two, patient data not explicitly part of the patient's legal medical record as defined by the healthcare organization. This record will then vary by organization as the definition of a patient's legal medical record can vary by healthcare organization. This variation can include items such as information purchased about past medical claims, dietary and exercise information as well as other relevant medical data available from external non-organizational sources like health insurance claims history. This information allows healthcare organizations to create a detailed and holistic record of a patient's health. However, this large aggregation of personally identifiable patient data raises serious privacy and security concerns amongst those about whom the data is collected – the patients (Linden et al. 2009; Patel et al. 2015).

In an attempt to address consumer privacy and security concerns regarding patient-centric health data, the US government passed two acts; The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and The Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH). When the first act passed, HIPAA required the Secretary of the U.S. Department of Health and Human Services to develop regulations protecting the privacy and security of certain health information, now commonly known as the HIPAA Privacy Rule and the HIPAA Security Rule (Secretary, HHS. O. 2013). The Privacy Rule, or *Standards for Privacy of Individually Identifiable Health Information,* establishes national standards for the protection of certain health information, while the *Security Standards for the Protection of Electronic Protected Health Information* also known as the Security Rule, establishes a national set of security standards for protecting certain health information that is held or transferred in electronic form (Secretary, HHS. O. 2013). The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations known under the law as "covered entities" must put in place to secure individuals' "electronic protected health information (Secretary, HHS. O. 2013)." The second act passed by the US government, the HITECH Act of 2009, is intended to address the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules (Secretary, HHS. O. 2017). With respect to HIPAA and the privacy and security concerns of patient data, HITECH established the following; four categories of violations that reflect increasing levels of culpability, four corresponding tiers of penalty amounts that significantly increase the minimum penalty

for each violation, and a maximum penalty amount of $1.5 million for all violations of an identical provision (Secretary, HHS. O. 2017). However, both acts do not state “how” a healthcare organization should enact these rules and regulations; they only address “covered entities.” The acts apply to “electronic protected health information (Secretary, HHS. O. 2013).” Further, these acts do not explicitly take into account the actual privacy and security concerns of those affected, leaving healthcare organizations to handle any information and/or business practices related to these laws, at their own discretion.

When applying justification for a call to research in this area, two key elements are necessary, the industry perspective and the academic perspective. Both make a strong case for the cause of continuing research in the area of privacy and security in healthcare, but in different ways. From the industry perspective, healthcare privacy and security failures have run rampant, leading to a strong need for research into possible solutions. For example, HealthcareITnews.com (Davis August 2017), reports that in June 2017, Pacific Alliance Medical Center’s servers were hit by a ransomware attack and during the investigation officials said they couldn’t rule out whether 266,123 patient records were accessed, however it is now believed that these records may have been compromised. This has resulted in all patients whose records that may have been compromised being offered two years of free identity protection at the expense of Pacific Alliance (Davis August 2017). Pacific Alliance also took measures to enhance security measures to potentially avoid a repeat of this situation in the future, strengthening things such as virus protection (Davis August 2017). This type of data breach demonstrates a clear warning to other healthcare systems that they may be vulnerable to even simplistic attacks resulting

from inadequate basic protections like virus protection. Another example that illustrates the need for additional research in this area is an article from ModernHealthcare.com (Arndt, August 2017) that describes how healthcare data breaches are on the rise and that cybersecurity as a whole only represents a small fraction of healthcare IT spending. In 2017, cybersecurity breaches rose and outpaced those of 2016 according to figures provided by the Department of Health and Human Services and it is reasonably expected that this trend will continue into 2018 (Arndt, August 2017). Another difficult figure is that of healthcare IT cybersecurity spending, which serves to demonstrate the degree to which security is underdeveloped in this area. According to a survey conducted by the Healthcare Information and Management Systems Society, forty percent of respondents said that only 1% to 2% of their organizations' budgets goes to cybersecurity, and another 32% said 3% to 6% goes to cybersecurity (Arndt, August 2017). These types of figures and incidents raise the alarm in industry that greater focus on cybersecurity is necessary in order to address the onslaught on data breaches occurring every year.

From the Academic perspective, this work heeds calls for research focusing on design, action contributions, and supported by empirical evidence in the Information Systems literature (Belanger and Crossler 2011; Belanger and Xu 2015; Smith et al. 2011). Patient concerns around the privacy and security of information retained by healthcare organizations must be addressed through the development and implementation of effective policy that incorporates the concerns of the affected stakeholders, both at the governmental and organizational level (Belanger and Crossler 2011; Belanger and Xu 2015; Smith et al. 2011). Therefore, this research argues that any decision-making

process regarding the development of public policy intended to deal with concerns related to patient privacy and security should not only address regulatory concerns, but also patient-centric informational concerns.

In order to accomplish this goal, governments and healthcare organizations must first understand patient privacy and security concerns regarding information being stored by healthcare systems from those directly affected (Linden et al. 2009; Patel et al. 2015). However, understanding the concerns of patients is not enough; governments and organizations must also understand the way in which patients want their privacy and security concerns addressed. This includes both the way the meaning of the objective is interpreted (i.e. “maintain confidentiality” means enabling record level encryption while data is at rest) as well as the method by which patients prefer its implementation to take place. Further, it is important to understand how patients view their preferred ways of implementing such measures as compared to the current methods of doing so. Lastly, it is important for governments and healthcare systems to understand the patient-centric objectives necessary to maximize the privacy and security of data. However, once the objectives are understood, it is then important for healthcare organizations to have the ability to maximize those objectives as well as for government regulators to evaluate healthcare systems’ progress in doing so. Therefore, a mechanism is required by which the implementation of these patient-centric privacy and security objectives can be evaluated in the form of a decision model. This model will allow governments to evaluate both regulatory and patient-centric privacy and security objectives related to patient information stored by a healthcare system. Additionally it can serve as a self-diagnostic

tool by the healthcare system itself to assess its own progress and address gaps in its capabilities.

Hence, the three research questions are as follows: Firstly, what are the patient-centric objectives for addressing informational concerns surrounding the privacy and security of data stored by healthcare systems. Secondly, how are these patient-centric objectives optimized given varying security contexts and ethical dilemmas surrounding the use of such information. Lastly, how can the efficacy of healthcare systems' implementation of these given objectives, including regulatory concerns, related to the use of patient information in a given decision context be evaluated? To accomplish this task, Multi-objective decision analytic techniques are used to elicit patient-centric preferences to assist organizations and governmental institutions alike in dealing with their privacy and security concerns for defining policy. This research contributes to the field of Information Systems through improved strategic decision-making within organizations and government institutions related to the use of Information Systems. For example, by focusing on the actionable objectives and implementation scenarios most desired by the affected stakeholders, maximum value can be obtained while investing minimal finite resources. Specifically, the use of multi-objective decision analytic techniques, with Nissenbaum's (2004) contextual integrity as a normative framework, enables user-driven policy creation, implementation and enhancement by incorporating key privacy and security concerns specific to the use-case of the key affected stakeholders.

As the focus of this research is on the concepts of both Privacy and Security, it is important to contextualize what they are intended to mean and scope them properly for the purposes of this study. To begin, defining privacy is an extraordinarily difficult task due to its multidimensionality and broadness of potential scope, especially with respect to differences in academic research (Culnan et al. 2009; Smith 1993; Tsai et al. 2010) and lack of proper definition in healthcare (the term itself remains undefined in both HIPAA and HITECH). Therefore, to narrow this scope for the purpose of this research, privacy is thusly defined as, "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin & Ruebhausen 2015; Parks et al. 2011). Similar to the concept of Privacy, the definition of the term security can be equally ambiguous and/or broad in scope (Anderson 2003). While defining it could simply be to relate the core concepts of Confidentiality, Integrity and availability (CIA Triad), however a more practical definition is assumed. Hence, security is defined for the purposes of this study as, "A well-informed sense of assurance that information risks and controls are in balance (Anderson 2003, p. 310).

To this end, the remainder of this thesis is as follows: Firstly, a literature review is conducted that examines the prior literature surrounding patient privacy and security concerns around patient-centric data storage by healthcare systems. Secondly, a theoretical framework is proposed that can be used to provide a normative framework for understanding the patient privacy and security context in US based healthcare. Thirdly, the proposed methodology for this research, Value-focused Thinking, the Public Value

Forum and Multi-objective Decision Analysis modeling, is explicated. Fourthly, each phase is conducted with the results then analyzed. Lastly, a discussion takes place to synthesize the results, elucidating critical understandings resulting from this work, and then concluding with a presentation of the limitations and future directions for this research stream.

Literature Review

Prior to the inception of the literature review, it is essential to acknowledge that the research contained in this thesis involves three distinct academic knowledge areas. These distinct knowledge areas serve as the intellectual basis upon which the argumentation of this research rests, providing both a foundational understanding of the concepts drawn upon for this thesis and demonstrating academic justification for the validity of this undertaking. These three knowledge areas, divided into sections, are as follows; general information systems privacy and security literature, patient-centric privacy and security literature and literature pertaining to the use of public values for decision-making.

In the first section, general Information Systems privacy and security literature is reviewed to serve as a demonstration of the need for actionable empirical privacy and security based research in this field. It does so by providing the historical context of the field and then identifies needs for future research by academicians. In the next section, patient privacy and security concerns related to the use and dissemination of patient-centric data are reviewed. While this topic has been well research in academia, the focus of such work has been to understand whether concerns exist and if so, what they might

be. To this end, a viable solution that seeks to address the concerns of those most affected through the effective use of policy has, to date, not been found or a viable solution proposed. In the final section, using public values in decision-making, prior academic literature is reviewed to demonstrate that using public values in the decision-making process is an acceptable method for solving complex problems, such as patient privacy and security concerns around the use of patient-centric data in EMR systems.

Therefore, the academic literature reviewed in this chapter will serve several purposes. Firstly, it will demonstrate that the literature to date has only sought to examine patient privacy and security concerns this in area. Secondly, these concerns do in fact exist and are an ongoing problem requiring a solution as current research has yet to propose tangible solutions. Lastly, it demonstrates that using public values to solve complex problems are an acceptable practice in the academic literature (Dhillon et al. 2016; Dhillon & Smith 2017; Dhillon & Torkzadeh 2006; Keeney 1990, 1996, Keeney 2006, 2013; Keeney and Palley 2013; May et al. 2013; Merrick & Garcia 2004; Merrick et al. 2005a; Merrick et al. 2005b; Witesman & Walters 2014).

General Information Systems Privacy and Security Literature

Research regarding the concepts of privacy and security within the Information systems literature is highly diverse across a spectrum of contexts. However, there are several seminal literature reviews within the field that clearly aggregate the importance, direction and needs regarding the future of both privacy and security research within the discipline

(Baskerville 1993; Belanger and Crossler 2011; Belanger and Xu 2015; Dhillon and Backhouse 2001; Smith et al. 2011). For example, both Baskerville (1993) and Dhillon and Backhouse (2001) discuss and review the security context in relation to the development of the field and the socio-technical interactions of organizations and Information Systems. In each, security is an important aspect of Information Systems that has been under-researched and is in need of consideration to ensure the proper development and management of Information Systems. Their reviews highlight the historical context for the development of the field as well as the progression of research to tend towards the purely technical aspect of information security, overshadowing needed development in other areas of Information Systems Security research. Directly pointing to this fact, Dhillon and Backhouse (2001) make a pointed call for research focusing specifically on socio-technical interactions, including but not limited to, the development of policy to manage such contexts relating to information security in organizations.

Likewise, seminal reviews of Information Systems literature regarding Information privacy, referring to the desire of individuals to control or have some influence over data about themselves, has been found to be lacking (Belanger and Crossler 2011; Belanger and Xu 2015; Smith et al. 2011). As continued advances in information technology raise concerns about information privacy and its effects, Information Systems researchers have been motivated to explore information privacy issues, including technical solutions to address these concerns (Belanger and Crossler 2011). Reviews by Belanger and Crossler (2011) and Smith et al. (2011) found that information privacy is a multilevel concept, yet

it is rarely studied in such a manner, often providing findings that have limited generalizability. It has been found that IS literature conducted in this area tends to focus exclusively on explaining and predicting theoretical contributions, with very few studies in journal articles focusing on design and action contributions (Belanger and Crossler 2011; Belanger and Xu 2015; Smith et al. 2011). To this end, calls for research on information privacy have been made, seeking more design and action information privacy research to be published in journal articles (Belanger and Crossler 2011). Additionally, Smith et al. (2011) state that while there are many theoretical developments in the body of normative literature and purely descriptive studies that have not been addressed in empirical research on privacy, rigorous studies that either trace processes associated with, or test implied assertions from, these value-laden arguments could add great value to this body of Information Systems research.

Patient Privacy and Information Security Concerns

In the academic literature, a great deal of research (See Table 1) has sought to examine the privacy and security concerns of consumers related the patient-centric health information stored in EMR systems (Angst et al. 2006; Bansal et al. 2010; Bourgeois et al. 2015; Campbell et al. 2007; Gordon et al. 2017; Sankar et al. 2003). However, to date there has yet to be any research conducted that actually worked to address these observed concerns based on the values of those affected. While no work has been done to date using the patient-centric values regarding the privacy and security of health data in EMR systems, it is important to review prior literature that both establishes these concerns exist

and demonstrate the call for action to solve them (Bourgeois et al. 2015; Gordon et al. 2017).

The academic research relating to patient-centric concerns tends to fall in one of three general categories: the confidentiality of identifiable patient health information, consent to use of patient data and lastly, patient perceptions of technology-related security concerns. For example, a survey of past academic research on the confidentiality of patient health information by Sankar et al. (2003) researched four broad conclusions: (1) patients tend to strongly believe that their information should be shared only with people directly involved in their care, (2) patients do understand the need for information sharing among physicians, yet HIV patients are less likely to approve the sharing of personal health information, (3) a large number of patients who agree to information sharing among physicians reject the idea of releasing information to third parties, including employers and family members, and (4) the majority of patients who have undergone a genetic testing procedure believe that patients bear the responsibility of revealing test results to other at-risk family members. It is important to note that the body of research from which these conclusions were drawn focused almost exclusively on the use of identifiable or potentially identifiable information by others outside of immediate health providers (Sankar et al. 2003). However, this category of research helps to establish the understanding that patients have long-standing concerns regarding the privacy and security of patient-centric data and sharing such data with anyone other than their physicians. Additional research by Bourgeois et al. (2015) in reviewing patient privacy with respect to how data is stored by health systems found that several deficiencies in the

current constructions of PHRs and EHRs need to be addressed. For example, EHRs have not been suitably designed to allow all types of information that require special consideration to be flagged as sensitive, whether automatically by predetermined logic or individually as specified by a provider. Second, PHRs must be designed with different access roles, so that users may have different views of the data based on what categories of data they are permitted to view (Bourgeois et al. 2015).

Another important category that serves to establish the need for this research is the work of Bansal et al. (2010), who developed a set of constructs based on both utility and prospect theory as precursors to the formation of trust and the privacy concerns that impact users' personal temperament with respect to the disclosure of their personal health information to online health websites. Bansal et al. (2010) found that, with respect to consent, patient's current health status, personality traits, culture, and prior experience with websites and online privacy invasions played a major role in their degree of concerns and willingness to consent. Conversely, a mail-based survey using adult patients in England conducted by Campbell et al. (2007) found that roughly 28–35% of patients are neutral to their health information. For example, information such as age, gender, ethnicity, reason for treatment, medical history, personal habits impacting health, type of treatment obtained, side effects of treatment, being used by physicians for other purposes were apparently viewed indifferently. Interestingly, the researchers discovered that only 5–21% of patients expect to be asked for permission to use their information by physicians and about 10% of the patients expect to be asked for permission if their doctors used their health information for an array of purposes. These other purposes

could include the following; combining data with other patients' data to provide better information to future patients, sharing treatment outcomes with other physicians, teaching medical professionals and writing research articles about diseases and treatments. This information is important for two reasons; firstly, it establishes that a level of concern does exist with respect to consent related to the use of patient health information for various purposes, and secondly, it demonstrates that consent to use is an important aspect with respect to patient privacy and security concerns.

The last category in this area deals with patient security and privacy concerns related to the advancement of technology in patient record keeping systems. In a study by Angst et al. (2006), researchers investigated the divergence of perception among patients towards different types of personal health record systems, specifically in an increasing order of technological advancement. Their work included various mediums of technology such as paper-based, personal-computer-based, memory devices, portal and networked PHR systems (Angst et al. 2006). The work found that patients' relative perception of privacy and security concern increased with the level of technology, meaning that as the use of technology increased, patient's privacy and security concerns tended to increase. Currently, work by Gordon et al. (2017) point to the fact that threats to patient data from the technology perspective still persist and are in fact growing in severity. These threats can take down entire systems, compromise patient data and result in undue harm to those the health system is trying to help (Gordon et al. 2017). These works are pertinent to our research efforts as healthcare organizations are implementing and have implemented

highly advanced data systems and features that present new or unknown privacy and security risks.

The Gap in Healthcare Related IS Privacy and Security Literature

There is a great deal of literature related to the concept of both privacy and security (See Table 1), however its focus tends towards traditional Information Systems (IS) concepts and traditional IS realms. By performing a comprehensive review of the IS literature and reviewing recent works whose purpose is to point out underdeveloped areas of privacy and security research (Lowry et al. 2017), two clear gaps in the IS literature appear; First, while there is a wide array of privacy and security research done in the field of IS, a number of opportunities exist in areas of growing interest such as Big Data (Lowry et al. 2017). Second, some research has been conducted in the field of IS in the realm of healthcare, however it overwhelmingly focuses on technology or concepts such as consent and identity management. Little to no work is being done as it relates to defining proper means of implementing policy to address lingering privacy and security concerns as it relates to data in the realm of healthcare. Hence, this research both fills a need for work to be done in this context and addresses an obvious gap in the academic literature as it relates to healthcare.

As an example, Lowry et al. (2017) performed a comprehensive analysis of the IS literature with respect to privacy in the field and developed categorical designations known as “artefacts,” which represent different aspects of IS privacy (and often security)

research. In Lowry et al. (2017) the purpose of these categories were to highlight current research trends over the last 10 years and highlight underdeveloped areas for new streams of IS research. With respect to the research in this study, five of the "artefacts" or categories, apply and are as follows; ethics, information, legal, organizational, and process (Lowry et al. 2017). Each category applies to a different aspect of IS privacy (and security) research, such as the information artefact, which contains research that talks about the nexus of information and privacy and security (Lowry et al. 2017). This is important as Lowry et al. (2017) demonstrates that research related to Data privacy and security fall within this category and at present is underdeveloped. Pointing to select articles (Cram et al. 2017; D'arcy et al. 2009; Siponen and Willison 2009; Wall et al. 2016), Lowry et al. (2017) demonstrate these streams of IS research are underdeveloped at this current point in time and represent opportunities for research such as this, addressing areas of legal concern, data use and patient privacy and security concerns related to this different dimensions of healthcare-related research in the field of IS. This is also due to the fact that (See Table 1), very little IS research focuses on healthcare at all when addressing the concepts of privacy and security. Further, any IS work that does deal with concepts of privacy and security in the IS field tend to focus on similar concepts such as consent (Cambell et al. 2007), patient identity management (Angst et al. 2006; Brisson et al. 2015) or technology related concepts (Burns et al. 2016).

For this reason, understanding patient privacy and security concerns related to storing health information in such advanced systems becomes critical to ensuring healthcare organizations can establish trust with their patient populations by adequately addressing such concerns. In the next section, academic literature will be examined that explores the use of public values as a means of solving complex problems such as this one, by incorporating stakeholder values into the decision-making process for developing effective public policy aimed at addressing a particular decision-context.

Perspectives	IS Literary Works	Central Research Issues
Generic IS Security and Privacy Concerns	Algarni et al. 2017; Anderson et al. 2017; Bansal and Gefen 2015; Baskerville 1993; Belanger and Crossler 2011; Belanger and Xu 2015; Boss et al. 2015; Bulgurcu et al. 2010; Burns et al. 2017a; Burns et al. 2017b; Chen et al. 2011; Chen et al. 2012; Choi et al. 2015; Cram et al. 2017; Crossler et al. 2013; Crossler and Posey 2017; D'arcy et al. 2009; Dhillon and Backhouse 2001; Dinev et al. 2013; French et al. 2014; Garba et al. 2015; Gerlach et al. 2015; Goel et al. 2017; Greenaway et al. 2015; Herath and Rao 2009a; Herath and Rao 2009b; Hsu et al. 2015; Hu et al. 2011; Hui et al. 2007; Johnston and Warkentin 2010; Johnston et al. 2016; Karjalainen and Siponen 201; Keith et al. 2013; Kim et al. 2010; Kokolakis 2017; Lee et al. 2016; Lowry et al. 2017; Lowry and Moody 2015; Lowry et al. 2015; Miltegen and Smith 2015; Myyry et al. 2009; Paquette et al. 2010; Pavlou 2011; Siponen et al. 2007; Siponen and Willison 2009; Smith et al. 2011; Son 2011; Spears and Barki 2010; Straub Jr. 1990; Sumner 2009; Tsohou et al. 2015; Wall et al. 2016; Wang et al. 2015; Warkentin and Willison 2009	Confidentiality, Integrity and Availability of data, Socio-Technical Security, Empirical Research, Privacy Assurance, Compliance, Security Risk Management, Security Policy
Healthcare Privacy and Security Concerns in IS	Angst and Agarwal 2009; Angst et al. 2006; Bansal et al. 2010; Bourgeois et al. 2015; Brisson et al. 2015; Burns et al. 2016; Campbell et al. 2007; Gordon et al. 2017; Kordzadeh 2017; Kwon and Johnson 2014; Li and Qin 2017; Sankar et al. 2003	Individual Identity management, personal privacy, Medical Record Protection and Consent
Applicable Legislation	HIPAA + HITECH Acts	Concern for patient privacy; Ensure compliance

Table 1. Summary of Patient-Centric Privacy and Security Research

Using Public Values for Decision-Making

The practice of incorporating public values into the policy-making decision process has a robust basis in the academic literature, where the public's opinion is intended to drive policy creation and implementation (Dhillon et al. 2016; Dhillon & Torkzadeh 2006; Keeney 1996, Keeney 2006, 2013; Keeney and Palley 2013; May et al. 2013; Merrick & Garcia 2004; Merrick et al. 2005a; Merrick et al. 2005b; Witesman & Walters 2014). The opinion of the public is driven by the inherent values of the collective individuals and is very useful for creating policy that is both effective and accepted by those affected through its implementation (Keeney 1996, 2006; Dhillon et al. 2016; Dhillon & Torkzadeh 2006). Due to the aforementioned benefits, public values are an important consideration within policy decisions and should be incorporated into the decision making process, despite being a difficult task (Dhillon et al. 2016; Dhillon & Torkzadeh 2006; Keeney 1996, 2006; Witesman & Walters 2014). The uses for all forms of patient-centric data in healthcare is growing rapidly, giving rise to new privacy and security concerns for those about whom the data is being collected. These concerns include things such as; Breach notification, consent, data transfers and security of information stored by healthcare systems (Meingast et al. 2006; Martínez-Pérez et al. 2015). Current policies do not adequately account for these concerns as the can be broadly interpreted and applied, hence they cannot adequately address privacy and security concerns of all affected stakeholders.

In order to develop comprehensive policy that can address the privacy and security concerns of all involved stakeholders, their values must be elicited and incorporated into the decision-making process. For example, the seminal literature regarding the use of public values in the decision-making process is that of Keeney et al. (1990), who used the Public Value Forum technique to conduct two public value forums with selected members of the West German public. This was done to elicit values relevant for setting long term energy policies using input from the most affected stakeholders (Keeney et al. 1990). The purpose of conducting these value forums is twofold; firstly, to examine the feasibility of eliciting values from laypeople and combining them with factual assessments of experts, determining the extent to which values elicited formally conflict with values elicited informally, and secondly, to assess the advantages and disadvantages of the public value forum technique in solving complex decisions (Keeney et al. 1990). Dhillon and Torkzadeh (2006), who used public values to explore the concerns of organizations around the concept of information systems security. The authors developed nine fundamental and sixteen means objectives that were useful in understanding, from the perspective of the affected stakeholder, what was necessary for organizations to ensure the security of their information systems (Dhillon and Torkzadeh 2006). Another example is that of Dhillon and Smith (2017), who explore the topic of cyberstalking prevention. Dhillon and Smith (2017) use Keeney's Value-Focused Thinking (1992) technique to extract latent societal norms in the cyberstalking context to help develop actionable objectives aimed at developing cyberstalking prevention methods by government institutions through the implementation of effective public policy.

Value-focused Thinking versus Analytic Hierarchy Process for Decision-Making

While Value-focused Thinking was selected as the methodology for conducting research in this study, another prominent means of facilitating decision-making exists, known as Analytic Hierarchy Process or AHP (Saaty 1980). The analytic hierarchy process (AHP) is a structured technique for organizing and analyzing complex decisions developed by Thomas L. Saaty in the 1970s, with particular application in group decision making (Saaty 1980). Saaty (1980) contends that rather than prescribing a "correct" decision, the AHP helps decision makers find one that best suits their goal and their understanding of the problem by providing a comprehensive and rational framework for structuring a decision problem as well as for representing and quantifying its elements, for relating those elements to overall goals, and finally to evaluate alternative solutions.

However, while AHP is a commonly used decision analysis technique, is not appropriate for modeling decision problems in the face of uncertainty (Belton, 1986), and additionally suffers from a flaw within the ranking procedure, often referred to as rank reversal, which acts as an underlying symptom of a larger problem, that rankings produced by AHP are arbitrary in nature (Dyer 1990). Additional research conducted recently also demonstrates that AHP does not generate stable preferences (Lienert et al. 2016) as AHP uses ratio-scale to elicit decision makers' preferences, which is not suitable for value-based judgments and requires manual corrections for the problem of rank reversal (Dyer 1990). Value-focused Thinking uses interval scale and provides guidelines to elicit decision makers' preferences and thus overcomes the limitations of AHP

(Keeney 1992; 1994a; 1994b). This reasoning justifies the use of the Value-focused Thinking technique as an effective means to design a value-based approach, while satisfying laws in the problem environment for this research (Hevner et al. 2004).

Theoretical Framing

In order to properly contextualize the findings of this research, a theoretical framework is necessary, as it provides a normative framework for grounding and interpreting the actionable objectives generated in this research,. For this study, Nissenbaum's (2004) contextual integrity is selected as it provide two key mechanisms for advancing Keeney's (1992) Value-focused thinking process; First, it provides a means of checks and balances to use while converting values to actionable objectives, ensuring the goal of those objectives remains true to its intended purpose. Second, it provides an interpretive mechanism for understanding and relating such learning to the broader academic and practitioner community. In this section, Nissenbaum's (2004) contextual integrity will be explained in greater detail as well as how it is integrated into this study to fulfill its intended purpose.

According to Nissenbaum (2004), contextual integrity is a theoretical framework that takes account of societal norms of appropriate information flows in terms of the transfer of personal information amongst various agents. Instead of simply proposing it as a working definition of what these norms are or should be, it is intended to be used as a normative model to contextualize a particular concept (Barth et al. 2006). The purpose of this normative model is to evaluate the flow of information between what are known as

"agents," which can be either individuals and/or other entities (Barth et al. 2006). The model of contextual integrity operates by placing particular emphasis on explaining why certain patterns of information flow provoke public outcry while others do not (Barth et al. 2006). This is an important concept for our research as we are concerned with how to manage the societal norms of information flows with respect to managing privacy and security concerns related to the use of patient-centric information by healthcare systems.

To this end, societal values (public values) will be elicited by combining contextual integrity as a normative model with Keeney's (1992) Value-Focused Thinking, to make explicit the norms or rules that govern people's perceptions of how privacy and information concerns should be addressed with respect to the informational use of patient data by healthcare systems (See Figure 1). Using contextual integrity to guide the methodological aspect of our research facilitates the extrication of an intricate system of social norms governing information flow surrounding patient-centric data used by healthcare systems. These social norms can serve as a basis for understanding the normative commitments for ensuring the privacy and security of patient data in order to operationalize these norms in guiding public policy decision-making. Therefore, Contextual Integrity can be used as a normative model to help define actionable objectives aimed at the ensuring the privacy and security of patient data, which are then operationalized using Keeney's (1992; 1999, Keeney et al. 1990) Value-focused Thinking and Public Value Forum techniques.

According to Nissenbaum (2004), contexts in contextual integrity are important as they offer a platform for a normative account of appropriate information flows, which determine and govern key aspects such as expectations, behaviors, or limits. When considering contextual integrity, there are two types of informational norms that are integral; norms of appropriateness, and norms of distribution (Nissenbaum 2004). According to Nissenbaum (2004), contextual integrity is maintained only when both types of norms are upheld, and consequently it is not upheld if either of the norms is violated. Hence, the benchmark of whether objectives will facilitate protections of a patient's privacy and security related to the use of patient information by healthcare systems is contextual integrity, in relation to the norms of appropriateness and distribution amongst of sample of participants. To qualify this benchmark, norms of appropriateness and distribution will be detailed further to demonstrate their proposed application to this research.

For Nissenbaum (2004), norms of appropriateness dictate what information about a person is appropriate to reveal in a particular context, such as when using patient health data contained in healthcare information systems. The norms of this particular context place limits on the type or nature of information about various individuals that is allowable, expected, or can be demanded to be revealed (Nissenbaum 2004). For example, patients may expect their physician to confer with colleagues in order to provide greater continuity of care; however, simply discussing a difficult or interesting patient case with no intention of gaining assistance from a colleague may not be considered a socially acceptable behavior when the context is considered. For this reason,

it is important that we draw out these norms of appropriateness in the context of the proper use of patient-centric health data by healthcare systems to form actionable objectives, which can then be used to prevent violations of contextual integrity on these grounds.

The second norm that is important for this research when assessing contextual integrity is the norm of distribution, which is the movement, or transfer of information from one party to another or others (Nissenbaum 2004). Equally important to this work is the question of how the flow of information can be managed in the context of patient information security to ensure contextual integrity and minimize scenarios that would cause violations. This means that the appropriateness of information is not all that matters in this context, as its distribution must follow contextual norms of information distribution (Nissenbaum 2004). As an illustration, it is generally assumed that when someone is given privileged access to confidential information it will stay as such. Yet organizations may violate this agreement by using patient information in a way that can be viewed as damaging to the privacy and reputation of the person violated in this manner. Hence, actionable objectives developed by this research will be guided by both of these types of norms to use contextual integrity as a normative framework to ensure the protection of patient-centric data stored by healthcare systems.

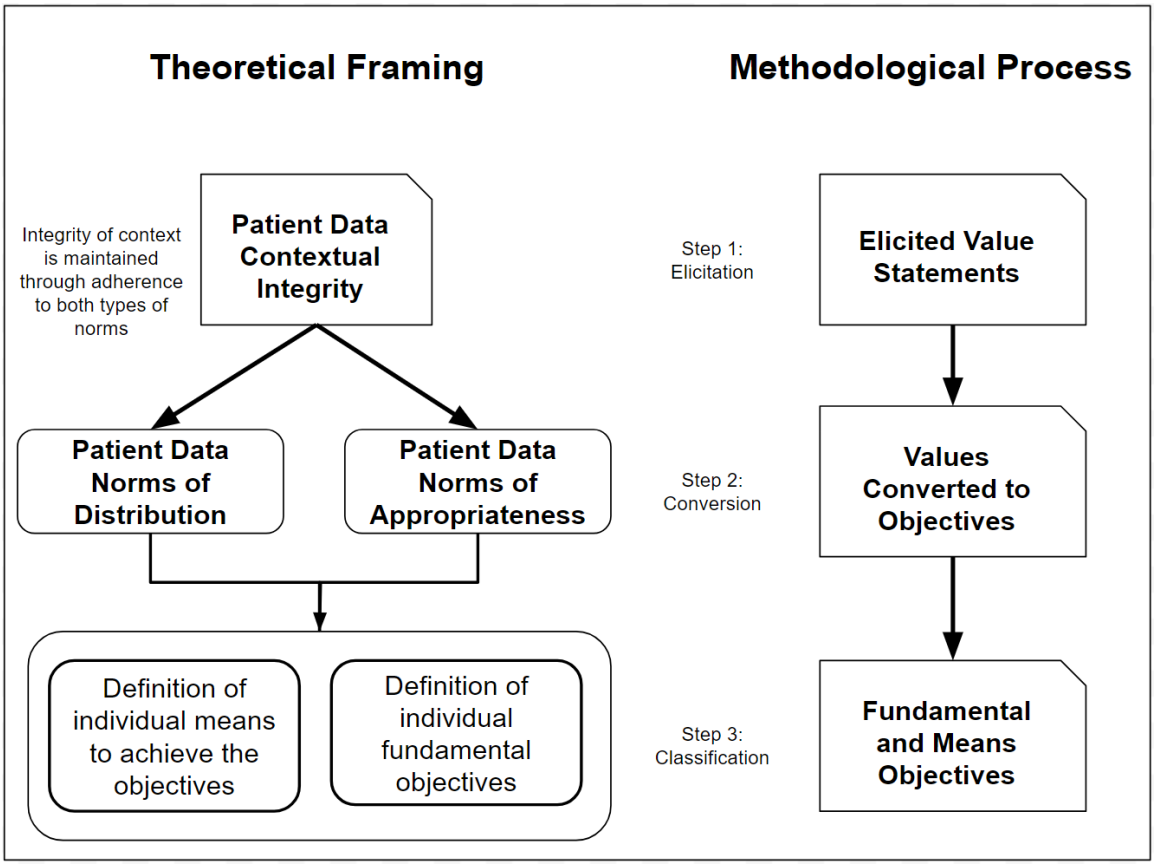

Figure 1. Theoretical Framing

The Methodology

While public values are important, aiding in making policy decisions, it is still unclear how policy makers should interpret public values for a specific policy context (Dhillon et al. 2016; Dhillon & Torkzadeh 2006; Keeney 1990; 1996; 2013). According to Keeney (1990; 1996; 2013; Dhillon et al. 2016; Dhillon & Torkzadeh 2006) this includes things such as; how public values should be operationalized to create policy, what role context-experts and their values should have in this process, and how expert recommendations and value interpretations can be combined in policy development process. Additionally, it should be noted that these aforementioned issues become more complex as the policy

context increases in scope and the problem domain increases in complexity (Dhillon et al. 2016; Dhillon & Torkzadeh 2006; Keeney et al. 1990; Keeney 1996, 2013). To facilitate this process under complex conditions, several approaches exist to shed light on and help to clarify the public values of complex policy problems such as surveys, indirect and direct value elicitation, focus groups and public involvement (Dhillon et al. 2016; Dhillon & Torkzadeh 2006; Keeney et al. 1990; Keeney 1996; 2013; May et al. 2013; Merrick & Garcia 2004; Merrick et al. 2005a; Merrick et al. 2005b). Table 2 illustrates the advantages and disadvantages of each method of eliciting public values.

Method of Value Solicitation	Advantages	Disadvantages
Survey	• Obtain Values in form of priorities among objectives, opinions about alternatives & preferences among alternatives • Non-Binding, but informative	• Hypothetical nature of questions • Influence of survey designer • Difficulty in designing, administering and Interpreting
Indirect Elicitation of Public Values	• No direct questioning necessary • Values inferred from behavior in marketplace • Can be applied outside of marketplace	• Some values may not have a market equivalent that can be observed • Questions are often hypothetical • Form of question can greatly influence outcome
Direct Elicitation of Public Values	• Interaction with individuals to elicit preferences and tradeoffs • Numerous methods exist for rating and weighting • Can improve tough policy decision making process	• Cost intensive • Time intensive • Hypothetical nature of questions
Focus Groups	• High amounts of relevant information is gathered • Adaptable and flexible format	• Groups often small and unrepresentative • Data is often anecdotal
Public Involvement	• Similar to Focus group, but has the intention of solving a particular problem • Goes beyond testing reactions	• Restricted to smaller problems • Places possible constraints on decision making

Table 2. Public Value Elicitation Methods (based on Keeney et al. 1990)

In this research, a combination of survey, focus group and direct value elicitation techniques is utilized in what are termed by Keeney (1992; Keeney et al. 1990) as Value-focused Thinking and the Public Value Forum. Using these techniques, we can examine the various fundamental and means objectives as well as the scenarios that can inform policy decision making by organizations and public officials in this context (Dhillon & Torkzadeh 2006; Keeney 2013; Witesman & Walters 2014). This is done by using a multi-attribute utility-based tradeoff procedure to elicit value-relevant information from interviews and focus groups to arrive at preferences for policy alternatives (Dhillon & Torkzadeh 2006; Keeney 1992; Keeney et al. 1990, 1996, 2013; Keeney and Gregory 2005). Initially in the process, interviews are conducted to determine the values that then allow for the creation of objectives and their attributes with respect the privacy and security of health-related data stored by healthcare systems (Dhillon & Torkzadeh 2006; Keeney 1988, 1992; Keeney and Gregory 2005). By using Value-focused Thinking to elicit the latent values that can be used to derive these objectives, a 'WITI test' (*Why Is This Important* test based on Keeney 1992) is performed to identify the fundamental and means objectives for ensuring the privacy and security of health related data. From this, the Public Value Forum presents scenarios that represent multiple policy implementation dimensions for evaluation. The purpose of this methodological process (See Figure 2) is then threefold; Via Value-focused Thinking, the Public Value Forum, and Multi-objective Decision Analytic techniques, to elicit public values about (1) the fundamental objectives necessary to ensure the privacy and security of health-related data in healthcare information systems, (2) assess multiple dimensions policy implementation,

and (3) develop a multi-objective decision making model to enhance the decision-making process of policy-makers in this context.

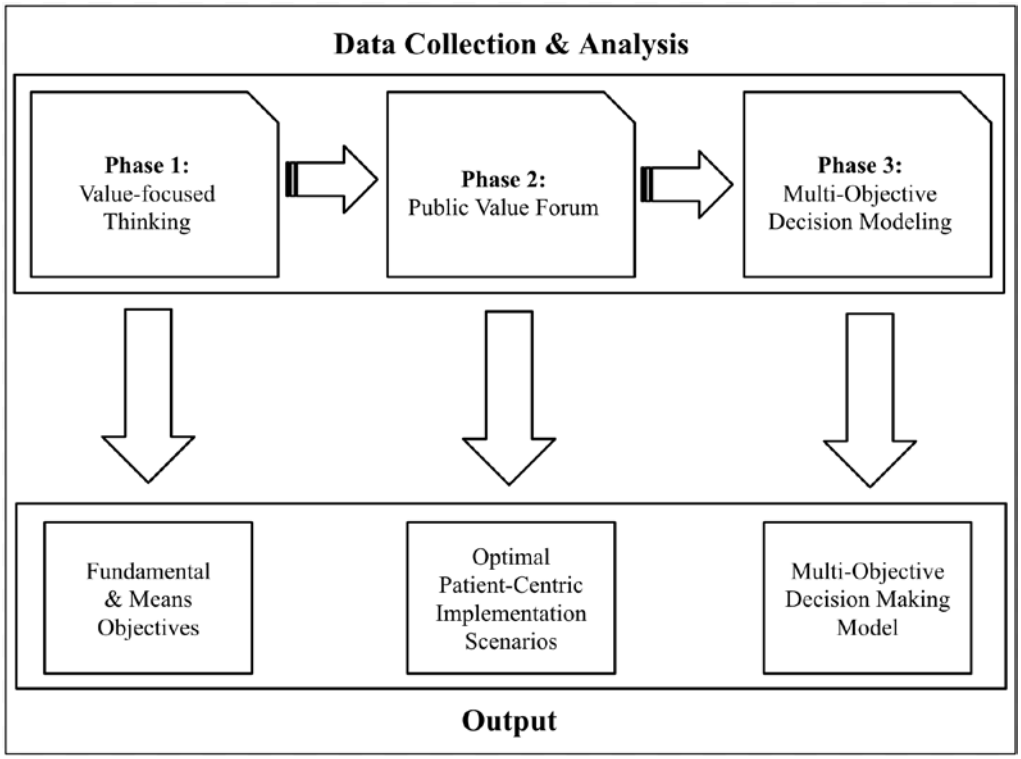

Figure 2. The Research Methodology

Phase 1: Value-focused Thinking

The following three-step process (See Figure 3) is used to identify and organize the values that an individual might have with respect to privacy and security of health-related patient data in healthcare information systems (Keeney 1992): Firstly, interviews are conducted which elicit the values an individual might have within a decision context. Secondly, individual values and statements are converted into a common value format,

such as an objective oriented statement. Then similar objectives are grouped together in order to form clusters of objectives. Finally, the objectives are classified as either fundamental to the decision context, resulting in a fundamental objective, or simply a means to achieve the fundamental objectives, which is known as a means objective.

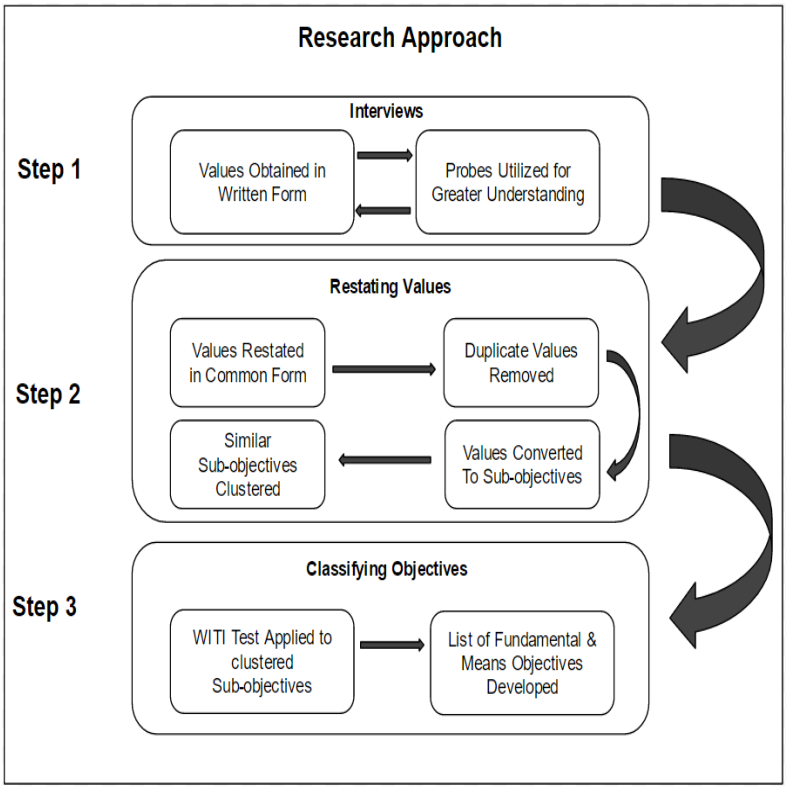

Figure 3. Value-focused Thinking Process

Identifying values

To begin, interviews are conducted with the concerned peoples as a process of identifying values. At the beginning of each interview, the purpose is clarified and context and scope of the interview are established. The core objective in this interview is to understand the

fundamental objectives for addressing privacy and security concerns related to patient data in healthcare information systems. To set the decision context, it is emphasized that the scope for eliciting these values is limited only to individuals, not organizations such as businesses or governments. After defining the scope of the interview, explanations are provided to the interviewee so that they can understand key terms such as "healthcare information systems," "patient data" and like terms, which helps to establish a common understanding of the terminology. It is made clear to respondents that the goal is to understand values that people might have with respect to the privacy and security of data retained by healthcare systems. To identify these values, several questions are posed about their personal values toward the privacy and security of patient-centric data. The starting-point questions were: What do you value most in protecting a patient's information in electronic medical records? What are your values regarding where the data should reside and why? What kind of tools do you think people want used to protect a patient's electronic data? All questions were open-ended. As individuals can express values differently, an inherent difficulty exists with the quiescent nature of the values, so different probing techniques are used to identify latent values. Keeney (1992), as probing techniques, suggests words such as "trade-offs" or "consequences" as useful in making such implicit values explicit.

Structuring values

Once the values are identified, a process of value structuring and objective development begins. Step one is that all statements are restated in a common form where duplicates are

removed. Then, common form values are considered from these statements and converted into sub-objectives. According to Keeney (1999), an objective is constituted of the decision context, an object and a direction of preferences, which in the case of this research is ensuring the privacy and security of patient-centric data. With all values systematically reviewed and converted into sub-objectives, it may be found that a number of sub-objectives deal with a similar issues, making it necessary to determine if these overlapping clusters should be merged or stand alone. By carefully reviewing the content of each of these sub-objectives, clusters are developed that group similar ones together (thus removing any overlap) and then each cluster of sub-objectives is labeled by its overall theme, which then becomes the main objective of the cluster.

Organizing objectives

The list of sub-objectives and corresponding clusters initially include both means and fundamental objectives so we must therefore differentiate between the two objective types. This is accomplished by repeatedly linking objectives through means–ends relationships, then specifying the fundamental objectives. To identify fundamental objectives, the question is asked, 'Why is this objective important in the decision context? (Keeney 1994).' If the objective is an essential reason for interest in the decision context, then the objective is a candidate as a fundamental objective. If the objective is important due its implications with respect to some other objective, then it is a candidate as a means objective. This is termed by Keeney (1994) as the 'WITI test.'

Phase 2: The Public Value Forum

The public value forum exists as a meeting of members of the general public, special interest groups or organizations that can last one to two days and usually involves anywhere between five and 25 participants (Keeney 1990; Keeney 2013). To begin, a policy problem is outlined, then the fundamental objectives relating to the problem are presented along with their particular attributes, and an objective value tree is created. 'Good' and 'bad' scenarios are created along with varying alternatives which can be presented to the value forum and discussed to find a preferable solution to the given policy problem (Keeney et al. 1990; Keeney 1996, 2013). The next step is to identify and select members from the general public to participate in the study to which Keeney et al. (1990) notes that there are two basic approaches. The first approach is that of the stakeholder approach where groups who have a specific stake in the outcome of any policy decisions are identified and asked to participate in the study. This can be especially useful when covering a controversial topic due to the emphasis on negotiation and conflict resolution (Keeney et al. 1990; Keeney 1996, 2013).

The second way for selecting study participants for a value forum is the representative approach where members of the public are selected at random which is most useful when little to no knowledge exists about reasonable public values to drive policy decisions (Keeney et al. 1990; Keeney 1996, 2013). Due to the relatively new nature and increased use of storing patient data by healthcare systems, little knowledge currently exists with respect to public values regarding patient-centric policy decisions, and therefore the representative approach was selected for use in this study. For this study, 2 groups of

stakeholders are involved in separate value forums representing privacy and security concerns for patient data storage, using both non-experts and substantive experts in the privacy and security of patient data to develop comprehensive multi-dimensional scenarios and analyzing them to better understand any potential differences between them. Next, once the forum participants are selected, the Objectives and Attributes are defined and appropriate contrasting multi-dimensional scenarios are evaluated that illustrate 'good' and 'bad' scenarios as well as varied alternatives of possible implementations of the defined objectives (Gregory and Keeney 1994). Lastly, the value forum is conducted to elicit public values regarding the decision context for policy decision-making and the results are analyzed.

The general structure of the value forum (See Figure 4) is (Keeney et al. 1990):

1. The policy problem is introduced and participants motivated
2. Objectives and attributes are defined and clarified
3. Ranking and Single-attribute utility functions elicited from all participants
4. Tradeoffs among the attributes are elicited from all participants
5. Construction of a Multi-Attribute Utility Models from results of all participants

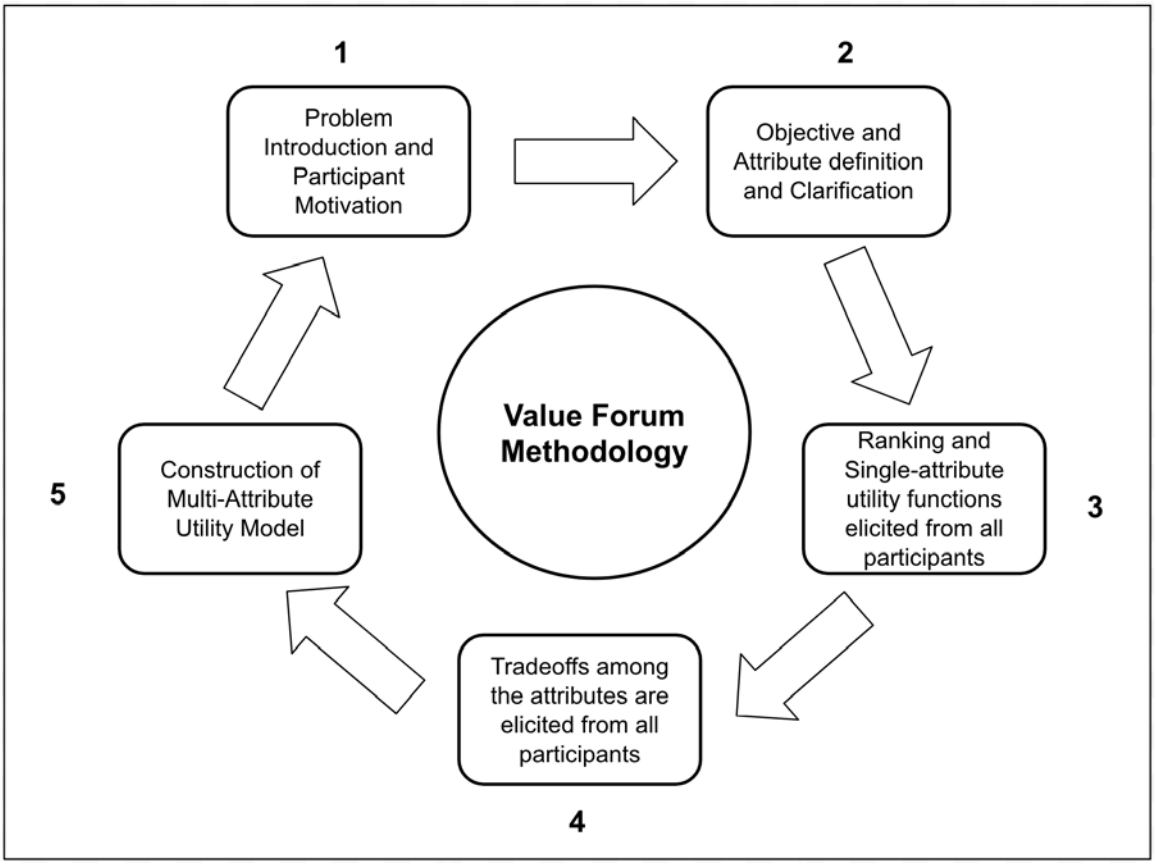

Figure 4. The Public Value Forum Methodology

The following is based on Keeney et al.'s (1990) work and describes what each step of the value forum is intended to accomplish:

1. *Introduction and Motivation*. To begin the forum it is important to provide participants with an understanding of the importance of using public value judgments in their decision making process. Participants are given an opportunity to ask any questions regarding clarification of the topic before moving on to stage two.

2. *Defining Objectives and Attributes*. Value-based objectives are defined among participants who are given a value tree for each objective with their corresponding attributes for clarification purposes. The multi-dimensional scenarios are also presented and clarified, as well as any participant questions answered before moving to stage 3 (Gregory and Keeney 1994).

3. *Ranking and Elicitation of Single-Attribute Utility Functions*. In stage 3 the quantitative levels of the attributes elicited may not be appropriate reflections of their relative desirability or utility. Therefore, utility functions are also used to demonstrate the relative desirability of a given objective or scenario. The choice of method depends on the purpose of the value forum and in many instances a simple rating method is sufficient.

4. *Elicitation of Tradeoffs*. Tradeoffs among attributes express the relative importance of attribute units by defining the exchange rate of one attribute unit vs. another. There are many methods for eliciting tradeoffs and relative importance information, such as swing weighting, and the choice of the appropriate method depends again on the policy context and the purpose of the value forum.

5. *Construction of a Multi-Attribute Utility Model*. The trade-offs elicited in step 4 are then converted into weights for the attributes using standard multi-attribute utility techniques (Keeney & Raiffa 1976; Keeney et al. 1990; Keeney 1996; Merrick et al. 2005a; Merrick et al. 2005b). For most value forums a multi-

attribute utility model is only a simple weighted average of the constructed single-attribute utilities. Researchers can perform additional tests to examine if a more complex multiplicative or multilinear model is necessary (Keeney & Raiffa 1976), if they find the additive model to be questionable. Should a researcher choose a more complex model, additional trade-off questions may be needed to elicit the additional parameters of the models. The multi-attribute utility model (also a value model, Keeney 1992; Akkermans & Van Helden 2002; Merrick et al. 2005a; Merrick et al. 2005b) is then used in combination with the expert evaluations to generate an overall model. The best way to describe the utility of this type of value model is to consider the various fundamental objectives as being O1, …On and m1 as a measure for a fundamental objective O1. It follows therefore that the vector m= (m1, m2, …, mn) would provide a description of a particular path in which a fundamental objective is delivered. The accumulated value of m would then serve as a measure (quantitative or qualitative) of the idiosyncratic resources and abilities that would fit the decision context (i.e. ensuring the privacy and security of patient data stored by healthcare systems). In the additive case (Keeney 1992), the overall utility *v* for any alternative described by *m1-mn* is

$$v = \left(m_1, m_{2,\ldots,} m_n\right) = \sum_{i=1}^{n} k_i v_i(m_i)$$

where *n* is the number of attributes, where k*i* is the weight ascribed to the objective O*i* and v*i* is the relative desirability scaling. From here, individual utility functions can be calculated for each participant. Once each individual utility is calculated a scaled weight can be applied to each individual function and the

result combined additively for a cumulative group utility function using the formula (Keeney 2013);

$$U_G(A_n) = \Sigma_m w_m U_m(A_n)$$

where U*G(An)* is the Utility of a group for a given alternative, which is equal to the sum of U*m*(A*n*), the utility of an individual for a given alternative, multiplied by the given scaled weight W*m*, and is relative to the given importance of a particular participant within the group.

Phase 3: The Multi-Objective Decision-Making Model

To ensure greater measures of protection with respect to the privacy and security of patient data in healthcare information systems, a multi-objective decision-making model can be developed, which utilizes patient-centric objectives for evaluating the efficacy of a healthcare system's efforts to maximize the privacy and security of data related to patients. This is where Keeney's (1992; 1996) Value Focused Thinking (VFT) for decision analysis can also be used to create an objective-based framework for healthcare organizations and other institutions to model the necessary objectives for ensuring the privacy and security of patient data. This model can then be used to assess the implementation of the given objectives and demonstrate gaps in their performance relative to the objective's goal acting as quantitative metrics for comparison (Merrick et al. 2005a; Merrick et al. 2005b). This process occurs in five basic steps adapted from Keeney (1992) and Merrick et al. (2005a; 2005b) and derives its objectives directly from

vested stakeholders and substantive experts as well as the necessary importance and swing weights to build out a proposed proof-of-concept model. Before this can be done, it is first necessary to discuss in detail the steps which will be undertaken during this phase of the research. It is important to note that this model will use fundamental objectives, which are defined by Keeney (1992; 1996) as "providing a structure for clarifying the values of interest in a given decision context and provide a basis for evaluating alternative."

The process for developing and quantifying an objective-based model involves the following steps (Keeney 1992, 1996; Merrick et al. 2005a; Merrick et al. 2005b; Merrick & Garcia 2004):

(1) Critical analysis of academic literature or generation of values through a value forum or survey and interview type methods, which is conducted by the analysts/researchers, to identify the factors that are fundamentally important as well as elicitation of any omitted objectives from subject experts. The analyst should ensure that important objectives are not omitted.

(2) The objectives are structured into a hierarchy that clarifies the differences between strategic and fundamental objectives and eliminates redundancies of objectives derived from sources elicited in step one.

(3) Subject experts define attributes for the objectives to clarify exactly what the objectives mean and to measure any possible consequences. The measurements also include importance and swing weighting for each objective in the model by the experts (Kirkwood 1997).

(4) Construction of a Multi-Attribute Utility Model. The trade-offs elicited in step 3 are then converted into weights for the attributes using standard multi-attribute utility techniques (Keeney & Raiffa 1976; Keeney 1990; Keeney 1996; Merrick et al. 2005a; Merrick et al. 2005b; Merrick & Garcia 2004). For most decision context a multi-attribute utility model is only a simple weighted average of the constructed single-attribute utilities. However, researchers can perform additional tests to examine if a more complex multiplicative or multilinear model is necessary (Keeney & Raiffa 1976), if they find the simple additive model to be questionable in application. Should a researcher choose a more complex model, additional trade-off questions may be needed to elicit any additional parameters for the model. The multi-attribute utility model (also a value model, Keeney 1992; Akkermans & Van Helden 2002; Merrick et al. 2005a; Merrick et al. 2005b; Merrick & Garcia 2004) is then used in combination with the expert evaluations to generate an overall model.

The best way to describe the utility of this type of value model is to consider the various fundamental objectives as being O_1, …On and m_1 as a measure for a fundamental objective O1. It follows therefore that the vector $m= (m_1, m_2, \ldots, m_n)$

would provide a description of a particular path in which a fundamental objective is delivered. The accumulated value of m would then serve as a measure (quantitative or qualitative) of the idiosyncratic resources and abilities that would fit the decision context. In the additive case (Keeney 1992), the overall utility *v* for any alternative described by m_1-m_n is:

$$v = \left(m_1, m_{2,\ldots,} m_n\right) = \sum_{i=1}^{n} k_i v_i(m_i)$$

where *n* is the number of attributes, where k*i* is the weight ascribed to the objective O*i* and v*i* is the relative desirability scaling.

(5) Assessing the value gaps of individual objectives based on the outcomes of the analysis. This identifies areas for improvement and allows a cost-benefit analysis to be performed to determine to most cost-effective areas to implement change and target finite organizational resources (Merrick et al. 2005a; Merrick et al. 2005b; Merrick & Garcia 2004).

Evaluation and Results

With the methodology and theoretical framing explained in detail, the following sections provide the evaluation and results for this study by phase. In each section, details are provided of the phases' evaluation process, results, and implications for the output. As

each phase is linked to the one preceding it, with the output being used as the basis for developing the latter, Phase 1 is analyzed first.

Phase 1: Value-focused Thinking

In order to achieve the research goals of this study, phase 1 starts by using Value-focused Thinking guided by contextual integrity to develop the fundamental and means objectives necessary for ensuring the privacy and security of patient data used by healthcare systems. To begin (Figure 3), a sample is selected for the interview process in step 1, and once all interviews have been completed then step 2 and 3 are completed. Once each step in the Value-focused Thinking process has been completed, phase 1 is concluded and phase 2 begins. In the following sections each step in the process is explained and the outcome of each step is detailed and lastly a means-end objective network diagram is presented.

Sample Selection

Within the literature, there is a significant amount of variance in the number of individuals that can be interviewed. As an example, Hunter (1997) used the interviews of 53 people from two different organizations to do a content analysis to elicit individual conceptions based on their values. Phythian and King (1992) used two managers who were experts in assessing tender enquiries to identify key factors and rules that influence tender decisions. Additionally, Keeney (1999) collected interviews from over 100 individuals to obtain their values to develop objectives that influenced Internet purchases.

More recently May et al. (2013) used value-based objectives developed from 103 individuals to assess the factors that influenced the success of the implementation process for enterprise resource planning systems. For Keeney (1994b; 1999), no explicit number is given as objective generation through value elicitation from all pertinent stakeholders should continue until redundancy from saturation occurs. The reason for this is that the technique was developed to generate responses that will naturally facilitate a convergence over time.

In this study, 70 persons of varying background and experience were interviewed. With each interview lasting an average of fifteen minutes, to identify general values for managing data within healthcare systems related to patient privacy and security. These persons ranged in age from 18 to 65 years old, included multiple ethnicities and races, and had a roughly even split between men and women, with slightly more women than men. For this reason, we believe all persons interviewed were typical of the region as they expressed similar idiosyncratic and logically homogeneous behavior. The interviews produced over 200 unique responses per survey question, at which point saturation occurred and no further interviews were conducted. To select our sample and conduct our interviews we used a systematic sampling technique, interviewing every 10th person over a period of three weeks. We selected four healthcare clinics in an urban medium to large-sized Atlantic coast city in the United States of America. The main advantage of using systematic sampling in our study is the assurance that the population of this given area will be evenly sampled (Pinsonneault and Kraemer 1993). This is why systematic sampling was chosen over simple random sampling as there exists a chance in simple

random sampling that the selection of subjects will become clustered and bias our sample (Pinsonneault and Kraemer 1993). However, while this is a strength of our sampling method, it does potentially allow for a lack of randomness is sample selection and for this reason we chose multiple locations over a period of 3 weeks. We believe that by doing so we maintained consistency, diversity and transparency is our sample selection for this study (Pinsonneault and Kraemer 1993). Once saturation was achieved and redundancy in responses occurred, the individual responses were re-classified into roughly 200 common form value responses. This allowed us to cluster these common form value statements into 50 sub-objectives which were then grouped into 5 fundamental and 10 means objectives. The following sections are a detailed explanation of the exact process used to obtain the fundamental and means objectives for our research as well as how contextual integrity was used to facilitate the classification process as a normative model.

Identifying values

To begin the process of using Value-focused Thinking guided by contextual integrity, interviews are conducted with the concerned peoples, referred to as stakeholders. This is done as a process for identifying and making their latent values with respect to norms of distribution and appropriateness explicit. At the beginning of each interview the purpose of our research, ensuring the privacy and security of patient data retained by healthcare systems, is clarified and context and scope of the interview are established. The core purpose of this interview is to elicit latent stakeholder values to facilitate the development of the fundamental objectives necessary for ensuring the privacy and security of patient

data retained by healthcare systems. For both Value-focused thinking and contextual integrity, establishing the context is critical for deriving useful objectives (Keeney 1999; Nissenbaum, 2004). To set a consistent decision context for all persons being interviewed, we emphasize that the scope for eliciting these values is limited only to the individual's preferences, not organizations such as a businesses or for governments. After defining the scope and establishing the boundaries of the interview, explanations and definitions are provided to the interviewee so that they can understand what key terms such as "healthcare information systems," "patient data" and like terms mean, which helps to establish a common understanding of the terminology. It is made clear to respondents that the goal is to understand values that people might have with respect to the privacy and security of data retained by healthcare systems. To identify these values several questions are posed about their personal values toward the privacy and security of patient-centric data. The starting-point questions were: What do you value most in protecting a patient's information in electronic medical records? What are your values regarding where the data should reside and why? What kind of tools do you think people want used to protect a patient's electronic data? All questions were open-ended. As individuals can express values differently, an inherent difficulty exists with the quiescent nature of the values, so different probing techniques are used to identify latent values.

Keeney (1992) suggests words like "trade-offs" or "consequences" as useful probing techniques in making such implicit values explicit. Therefore, the technique applied in this step is not a survey with close-ended questions, but instead an open-ended conversation with directed questions and various probing techniques used to elicit latent

values, regarding societal norms with respect to ensuring the privacy and security of patient data held by healthcare systems, in order to make them explicit. It is important to note that the questions as well as the conversational probes during the interview specifically address the concept of contextual integrity as a framework for this study. For example, by using contextual integrity as a framework in the formulation of questions and the probing responses, we are clearly attempting to draw out the underlying behaviors, expectations and limits of privacy regarding the norms of distribution and appropriateness in the context of patient privacy and security. Any responses that exist outside the scope of this decision-context are eliminated or redirected to ensure that each response is consistent with the intended parameters of this research. Within this step we received over 200 unique responses to each question posed, which are then used for the next step in phase 1.

Structuring values

Once the latent values are extracted and saturation has occurred, the process of value structuring and objective development then takes place. To begin, all value statements are restated into a common form where all duplicate statements are removed in order to ensure only unique statements are considered. The common form restatement process occurs by taking two statements of value from interviewees, varying in form but express the same latent value, and creating a single uniform statement that expresses the same meaning as the two aforementioned individual statements of value. After this process has occurred, the common form values developed from these statements are converted into

sub-objectives. With all values systematically reviewed and converted into sub-objectives, it may be found that a number of sub-objectives deal with a similar issues, making it necessary to determine if these overlapping clusters should be merged or stand alone. By carefully reviewing the content of each of these sub-objectives, clusters are developed that group similar ones together (thus removing any overlap) and then each cluster of sub-objectives is labeled by its overall theme, which will then become the main objective of the cluster. Contextual integrity is used to guide this stage as clustering and merging objectives implies that only similar value statements with consistent intended outcomes be placed together. It is imperative that each cluster be checked in the phase to ensure value statements addressing different norms of either distribution or appropriateness are not placed together. Each cluster is also reviewed to ensure its objective addresses a potential violation of a norm of either distribution or appropriateness, not both. While it is feasible that some overlap may naturally exist due to the nature of the elicitation process and the open-ended responses of the interviewees, in order to create clear and concise objectives aimed at ensuring the privacy and security of patient data, a clear delineation between the two types of norms must exist. This step resulted in the creation of 50 sub-clusters of value statements being derived from the 200+ unique statement responses found in step 1 of the value-focused thinking process as guided by contextual integrity for phase 1.

Organizing objectives

Initially, the newly created list of sub-objectives and corresponding clusters include both means and fundamental objectives, resulting in the need to differentiate between the two. While each cluster and the underlying values associated with them have all been created with contextual integrity as a framework to guide the process as well as being evaluated to ensure they address either a norm of appropriateness or a norm of distribution, not all objectives created in this process will be fundamental to the decision context. As stated previously, objectives are classified as either fundamental to the decision context, known as a fundamental objective, or they exist simply as a means to achieve the fundamental objectives, thusly known as a means objective. This distinction is important in Value-focused Thinking, as it will later facilitate the construction of a means–ends objectives network diagram (Keeney 1992). This is a value model representing both quantitative and qualitative relationships for which the purpose is to enable further insight into a complex situation and thereby complement intuitive thinking (Keeney 1992; Power and Sharda 2007). Therefore, the process of creating means and fundamental objectives is accomplished by repeatedly linking objectives through means–ends relationships and then specifying the fundamental objectives from this interaction. To clearly identify and delineate between fundamental and means objectives, the question is asked, 'Why is this objective important in the decision context? (Keeney 1994a).' If the objective is an essential reason for interest in the decision context, then the objective is a candidate as a fundamental objective. If the objective is important due to its implications with respect to some other objective, then it is a candidate as a means objective. This is termed by

Keeney (1994a) as the 'WITI test.' The researcher repeatedly uses this test until all clusters have been clearly identified as either means or fundamental with respect to the decision context. This process can take several hours, having a number of iterations, until all clusters have been categorized appropriately with the researcher reviewing their work to ensure the meanings of each objective has not been changed from the meaning of the values being interpreted.

Further this process is conceptualized in the study by asking each cluster if it is a means to achieving contextual integrity, by directly attempting to prevent violations of contextual integrity, or if it is only a means to an end in this regard. This is useful in terms of means and fundamental classification as it helps to clearly and concisely identify the purpose of an objective within the decision context. For example, in this step the objective "maximize patient privacy" is developed, which pertains to norms of distribution. Also, the objective "ensure confidential collection of patient data" which is developed, which similarly pertains to norms of distribution. When reviewing the second objective, however, it can be clearly seen that it is simply a means of enacting the first since it is only one means of ensuring the privacy of patients in a healthcare system, in dealing only with how sensitive information is collected. Therefore, at a fundamental level we should primarily be concerned with addressing "maximize patient privacy," as doing so will also address the means objective. Hence, by addressing these concerns in this manner we would prevent a violation of contextual integrity by maintaining a norm of distribution in the context of ensuring the privacy and security of patient data. The results from this final step in phase 1 were the creation of a total of 5 fundamental

objectives and 10 means objectives. These objectives are explicated in greater detail and linked to applicable academic literature in the following sections.

Objectives for securing patient data

In this section the fundamental (Table 3) and means objectives are presented (Table 4) with respect to how they collectively contribute to ensuring the privacy and security of patient data in healthcare systems in the final form of a network diagram (Figure 4). In our research we found fifteen total objectives: five fundamental objectives and ten means objectives. The fundamental and means objectives build the means-end network model which can act as a decision pathway to model different decision contexts for achieving the fundamental objectives. They also present additional research opportunities for modeling dependent and independent variables using techniques, such as structural equation modeling, to determine the effect these moderating means objectives have on the fundamental objectives.

Fundamental objectives

In the following section each fundamental objective is explained, linked to academic literature when applicable, and a quote of a value statement used in the formulation of the objective is provided.

FO1 Maximize Patient Privacy

Patient privacy has been a long standing issue in the medical field since the inception of electronic information systems to record and maintain patient data. In a seminal piece by Barrows & Clayton (1996), they review the early challenges, both positive and negatives, to patient privacy presented by the introduction and use of Electronic Medical Record (EMR) systems. While Barrows & Clayton (1996) conclude that these EMRs may indeed be more secure than traditional paper record keeping systems employed at the time, concerns regarding patient privacy bear merit and require redress. However, presently privacy concerns regarding patient data still exist, with works such as those by Brisson et al. (2015) pointing to ongoing problems that must be solved. Issues such as tracking patient data, broad access to medical records and ethical conflicts regarding the use of patient data are still relevant and lacking in reasonable solutions (Brisson et al. 2015).

While concerns regarding patient privacy in academic literature are highly prevalent, they were equally widespread within the feedback provided in the interviews conducted in this study. Nearly every participant interviewed mentioned multiple times, in various ways,

privacy as a critical concern regarding their data in healthcare systems. Whether it was related to control over disclosure or notifications when any data was transferred to a new source, privacy concerns were revealed by participants with a high degree of detail. Participants stated, “My personal data reveals very intimate details about my life and who I am. It’s very private information and I don’t want anyone having access to it without my express consent. I also want to know whoever accesses my information actually has a reason to see it.” Hence, statements such as this reveal that through various methods such as controls and notifications of disclosure like dynamic consent (Williams et al. 2015), they can serve to maximize patient privacy from a patient-centric perspective.

FO2 Maximize Security of Patient Records

Just as concerns over patient privacy were prevalent throughout our interview process, concerns regarding the security of those records went hand-in-hand for most people interviewed. After expressing their concerns over the privacy of their records many immediately began to detail concerns over records security. For example, one person stated, “If my records aren’t secure, how can they be kept private? Hackers easily could get my information and spread it anywhere they choose if healthcare systems don’t have the best security in place to protect my data.” Sentiments such as these are quite valid as numerous data breaches have been documented in academic research (Topol 2015; Patil & Seshadri 2014), which support this cause for concern. An alarming statistic regarding data breaches in healthcare systems, research has found that some 94% of healthcare systems experienced a breach in the last 2 years at the time of the study with expectations

that this number was unlikely to decrease (Topol 2015). To this end, many people interviewed expressed similar beliefs and offered numerous reasons as to why security was important as well as how it should be implemented. Many of these suggestions centered around technical controls that emphasized security measures such as multi-factor authentication techniques, Role-based Access Controls and the use of Encryption to protect all forms of patient data.

FO3 Maximize Training for Proper Data Handling

While maximizing the privacy and security of patient data through the use of technical controls is important to those we interviewed, it was recognized by a large proportion that technical controls alone cannot ensure the privacy and security of their data. To this point, interviewees suggested that people exposed to their data require proper training and certification as well as an ethical mindset for handling sensitive information correctly. Many value statements were made to the effect that all new employees should receive mandatory training before being allowed to handle patient data, irrespective of their line of work or the sensitivity of such data. Additionally, many people felt that these training programs should be done on an annual basis and re-certification made a core competency for employees within a healthcare system to continue in roles interacting with patient data of any kind. Respondents provided value statements such as, “Proper training is critical. The best security controls in the world won’t work if people don’t know how to use them right.” Various studies have also found this to be true, finding 39% of breaches occurred (Ponemon 2012; Kamoun & Nicho 2014) or that leaked

information was commonly a result of employee negligence (Johnson & Willey 2011; Kamoun & Nicho 2014). Hence, it is therefore important that healthcare organizations not only address privacy and security through technical controls or clear operational procedures, but they must ensure that employees are trained in the use of such tools and execution of given acts so that they are done correctly.

FO4 Maximize Patient Access to Medical Records

When interviewing participants about ensuring the privacy and security of patient data in healthcare systems, a large number indicated they wanted access to their medical records to take a proactive role in ensuring the privacy and security of their own data. Often times, respondents indicated that they wanted unrestricted access to view the records being kept about them, thus ensuring no data was being collected of which they did not approve. Also, based on this access, participants in our study indicated they would prefer to have the ability to terminate information held in their record that did not pertain to their medical care and presented unnecessary privacy issues. One value statement to this effect was, “If a healthcare system is using non-medical data to track me, sell things to me or otherwise keeping data not directly related to my treatment...I want the ability to have it removed from my records. If they don’t need it to treat me, they shouldn’t have it.”

While many organizations may be hesitant about sharing all the information collected about patients, research has shown that there are positive benefits to the organization and

that any risks are often relatively minor. For example, an initial study by Ross & Lin (2003) found that providing patients access to their medical records enhanced the doctor-patient relationship, while risks such as causing patient confusion or worry were minimal. However, the authors acknowledge that the supporting statistical information was limited in power and of low quality. Another more recently published paper by van der Vaart et al. (2014), found similar results with a high quality sample, with 44% of the sample feeling more involved in their care and with a greater degree of knowledge of their treatments. Hence, organizations do indeed benefit from allowing patients some access and control over the records being kept on them.

FO5 Ensure Secure Overrides for Patient Data Disclosure

While participants in this study demonstrated a clear desire to possess control over the use and disclosure of their information by healthcare systems, they recognized that there may be situations where disclosure is necessary and consent may not be obtained by the individual themselves. Additionally, it was recognized that certain use-cases which may require data disclosure should be exempt from some of these rules or obligations as they are simply part of the expected function of a healthcare system. For example, one respondent stated the following, “I don’t have the time or ability to micromanage approvals over who can use or what can be done with my data. Time can be critical, life or death, in healthcare and some things just need to be done at that very second.” Many respondents believed that clear procedures can be put in place to manage those specific use-cases to ensure that when a medically relevant emergency occurs, access to critical

data is automatic and not beleaguered by bureaucratic restraints. For this reason, Moulton & Kin (2010) promote the idea of ethical medical decision-making to drive behavior in such scenarios to ensure that both patient outcomes are optimal and their privacy and security are maintained throughout the process.

Fundamental Objectives for Ensuring the Privacy and Security of Patient Data

FO1 Maximize Patient Privacy Patient controls all data disclosure All patient Personal Health Information stripped from research or public disclosure No selling of any medical data to for-profit businesses to earn profit by healthcare organizations Patients notified of all data disclosures and access to their medical records	**FO2 Maximize Security of Patient Records** Multi-factor authentication required for access to patient records Access controls in place to limit unnecessary access of patient records (i.e. Role based access control) All electronically shared medical records must use encrypted communication All electronically stored data must be encrypted and stored in safe storage mediums
FO3 Maximize Training for Proper Data Handling All new employees receive mandatory training on patient privacy Annual training and re-certification required for all employees with access to patient data Organizations must have compliance programs in place Best practices training for IT/Security on newest security and privacy methods and protocols	**FO4 Maximize Patient Access to Medical Records** Patients have unrestricted access to view their own medical records Full disclosure of all data kept about patient by healthcare organization Patient can terminate or restrict use of non-relevant medical data by organization
FO5 Ensure Secure Overrides for Patient Data Disclosure Policies in place for emergency disclosure of Patient data Ensure tending physician has access to all necessary medical data Specifically defined use-cases for overrides All overrides must be documented in patient records	

Table 3. Fundamental Objectives

Means objectives

In the following section, the means objectives developed in step 3 of phase 1 are presented. While the fundamental objectives are critical to the decision-context for informing the decision-making process, means objectives serve only as a possible pathway leading to the ultimate fundamental goals. Hence, while the means objectives are important to this research, only an explanation of their meaning and an example value quote that led to their formulation is provided. Future research can explore these means objectives to better understand the relationships between them as well as their possible effects on the decision-making process in this context using the provided means-end network diagram (Figure 4).

MO1 Ensure Confidential Collection of Patient Data

In order to maximize patient privacy, Fundamental Objective 1 (FO1), one possible means that could lead to such a desired outcome is by ensuring that any data collected by healthcare systems is done so in a confidential manner. Participants believed that by collecting data in a manner that is confidential, there is less likely to be obvious breaches of patient privacy. One such example of this belief was the following value statement, “If someone is collecting my personal information, I want it to go directly into a secure system. I also don’t like writing it down...what happens to the paper copy when it’s put into an electronic system? I want to know as few eyes as necessary are seeing my

information." It is for this reason that, while this is clearly an objective of note, it is only a singular means to an end with multiple possible solutions.

MO2 Minimize Non-Essential Access to Data

Much like MO1, another possible means for maximizing patient privacy is by minimizing or eliminating all non-essential access to patient's data. Participants expressed a very clear desire that if a person doesn't have a reason to be accessing their data, access is limited or restricted. Many who participated in this study explained this sentiment by stating they feel only those directly in their medical care should be accessing sensitive information. One such person stated, "Why would a hospital administrator need to see my detailed medical record? That is between the doctors, nurses and myself." By expressing a clear desire for limited access, this means objective presents yet another possible avenue for achieving the overall fundamental objective.

MO3 Ensure Patient Knowledge of Data Disclosure

Participants in this study made numerous mentions related to concerns over what persons or entities may or may not have their information. Numerous people responded that one way of managing patient knowledge and access to their data was by ensuring they were made aware of various disclosures of information. For example, one participant stated, "If a hospital makes it clear who can access my data and tells me about important

disclosures, I don't think I'll be as worried about it." By ensuring people are notified of important disclosures regarding their sensitive data healthcare systems can then improve patient access and facilitate patient privacy and security.

MO4 Maximize Use of Encryption on Patient Data

The security of patient data held by healthcare systems was an important objective for participants in our study and one means of addressing security often suggested was through the use of encryption. While most respondents did not possess in-depth knowledge of encryption, they knew that it was a technical control which could be implemented to make data more difficult to steal and thus result in better overall security. Maximizing the security of patient data from the patient-centric perspective, encryption is an important and necessary tool as demonstrated by the Office of Civil Rights within the US Department of Health and Human services listing a lack of encryption as one of the top 5 reasons for HIPAA violations (Lee 2016). Hence, statements such as, "My data should always be encrypted and if it isn't, it is definitely at risk," are clearly backed by corroborating evidence that emphasize its role as an important means objective.

MO5 Minimize Sharing of Patient Data

Throughout the interview process, respondents repeatedly expressed their desire for maximizing privacy and one means for doing so that was consistently offered was to minimize unnecessary sharing of data. While access and sharing may be considered one

and the same in this regard, respondents expressed a different meaning when discussing sharing of data. In this context, it was felt that sharing of data meant moving data from the possession of the healthcare system itself to another entity. Those interviewed for this study often stated that sharing amongst medical entities, for example, to develop new treatments for illnesses would be acceptable, but sharing data to improve marketing efforts would not. Statements such as, "I only want my data shared if it directly benefits me, not just so the healthcare system can make money using it to drive their own agenda," support this means objective.

MO6 Limit Non-Essential Data Collection

Based on responses from interviews, this means objective may serve to not only lead to the successful outcome of a fundamental objective, but also other means objectives. By limiting what data is collected by healthcare organizations in the first place, it may be less likely that potential privacy and security issues arise. While there may be a great deal of data that a healthcare system could find of use, by limiting the scope of what is collected from the patient-centric perspective, privacy could be better protected and security measures like access controls and encryption easier to implement. Supporting this means objective are statements such as, "If healthcare systems only collected information my doctor needed to treat me instead of amassing anything they can get their hands on, I would think they could focus their security efforts better." Additional statements like the following, "It's easy to keep data private if you don't collect it in the first place," support the notion that it may also enhance privacy.

MO7 Ensure Regular Patient Data Training Updates

A common sentiment echoed in nearly every interviewed conducted was the idea that, while policy, procedure and technical controls may go a long way in ensuring the privacy and security of patient data in healthcare systems, a poorly trained employee could bring it all down. Things like ensuring employees are properly trained in data handling, access rights and information security were all points brought up by respondents. Additionally, many respondents felt that having trained security professionals to help handle difficult situations was important, something in which healthcare organizations are currently lacking (Lee 2016). Statements like, "Training is important. Without proper training even the best laid plans will probably fail," help to demonstrate this objective's use as a means to achieving the fundamental objectives in this study.

MO8 Ensure Mechanisms for Patient Data Release

Throughout the conducted interviews, the release of patient data was approached in numerous ways, however many respondents expressed the desire to possess the ability to control the release of data themselves. It was stated by a large number of people in this study that if patients were in charge of releasing their own information, by transferring it to a new doctor's office as an example, they would be far less concerned about potential breaches in privacy. To this end, statements such as, "If I had the ability to control the disclosure of my data, that alone would make me more at ease," may indicate

implementation of this means objective could lead to enhanced feelings of patient privacy and security.

MO9 Ensure Ethical Data Disclosure Practices

In the context of ensuring the privacy and security of patient data in healthcare systems, ethics was a common cause for concern. Many persons interviewed for this study noted that ethical considerations should play a large role in data-related decisions and that an ethical organization would likely do a better job protecting sensitive data. Statements such as, "If a healthcare system has a strong ethical foundation, I think they are more likely to do the right thing when it comes to my privacy when they share any data," support this objective as a viable means for enacting the fundamental objectives in this decision context from the patient-centric perspective.

MO10 Ensure Secure Access Portals to Patient Data

Whether attempting to enact FO4 or FO5, an important means to accomplishing those fundamental objectives is the use of secure access portals to patient data. Numerous respondents stated that they believed one of the single greatest points of vulnerability for their data was the point of access. Many felt uncomfortable with the idea of having access to any form of data unless they knew it was secure and could not be easily accessed by hackers or compromised while they are using it themselves. For example, one respondent stated, "I don't want to create more vulnerabilities by asking for access to my data unless

I know it's secure and can't be easily used to steal my data." This means objective then not only influences various fundamental objectives, but also other means objectives in this study. Hence, any organizations considering creating patient portals to view data, should have a high degree of security to ensure patients feel safe using them.

Means Objectives for for Ensuring the Privacy and Security of Patient Data	
MO1 Ensure Confidential Collection of Patient Data	*MO2 Minimize Non-Essential Access to Data*
MO3 Ensure Patient Knowledge of Data Disclosure	*MO4 Maximize use of Encryption on Patient Data*
MO5 Minimize Sharing of Patient Data	*MO6 Limit Non-Essential Data Collection*
MO7 Ensure Regular Patient Data Training Updates	*MO8 Ensure Mechanisms for Patient Data Release*
MO9 Ensure Ethical Data Disclosure Practices	*MO10 Ensure Secure Access Portals to Patient Data*

Table 4. Means Objectives

Means-end Objectives Network Diagram

After identifying both the fundamental and means objectives, Keeney (1992; 1999) suggests a network diagram (Figure 4) be created to illustrate their interaction with each other. The purpose of this diagram is twofold; firstly, it is used to demonstrate the flow of means objectives into the fundamental objectives, which they help accomplish. Secondly, it is a useful tool for enabling organizations to visualize the logical flow of objectives and formulate policy focusing on those related to each other in their network path, an example of which is provided below. In the diagram, the fundamental objectives, as

previously stated, are essential to the decision context of ensuring the privacy and security of patient data in healthcare systems, so they are listed to the right of the diagram and at the end of the network's flow. The means objectives are important to the decision context in itself, but as a way to achieving some other objective. This is demonstrated by (Figure 5) linking the means objectives that contribute to another objective and that are ultimately necessary for the fundamental objective to be achieved. Some means objectives are necessary or impact fundamental objectives directly, while others appear to impact other means objectives that then serve to impact a fundamental objective. It is important to note the interplay between means objectives themselves as well as between the fundamental objectives so that as research progresses in this domain, all aspects that influence the fundamental objectives are understood and given adequate consideration.

As the means and fundamental objectives are grounded in stakeholder values, representing the norms of distribution and appropriateness essential for maintaining contextual integrity, it provides a better opportunity for an organization or government to understand the social complexities related to the decision context from a societal perspective. In other words, because objectives form the basis for any policy planning exercise, an organization or government should view our framework as a guiding point for defining their own policy planning efforts with respect to patient data as they explicitly address the societal norms concerning its privacy and security. Therefore, a well-defined path aimed at this particular decision context would then not only help in the strategic creation of a comprehensive and effective policy, but also help in identifying alternative methods of implementation to achieve its core purpose (as suggested by

Keeney 1992). In short, the relationships between the means and the fundamental objectives would then help in sketching the paths of policy change to best achieve the goal by providing valuable insight into the decision context. One useful way this can be achieved is by using the network diagram to develop value models, which represent decision pathways for developing policy in a given decision context.

According to Keeney (1992), the means–ends objectives network can act as a value model representing both quantitative and qualitative relationships. The purpose of such a model is to gain insight into a complex situation and thereby complement intuitive thinking (Keeney 1992; Power and Sharda 2007). As previously stated in the methodology section, the best way to describe the utility of the value model is to consider the various fundamental objectives as being O_1, …O_n and m_1 (sub-objective) as a fundamental measure for a fundamental objective O_1. It follows therefore that the vector $m= (m_1, m_2, …, m_n)$ would provide a description of a particular path in the diagram in which a fundamental objective is delivered. The accumulated value of m would then serve as a measure (quantitative or qualitative) of the idiosyncratic resources and abilities that would fit the decision context (i.e. ensuring the privacy and security of patient data in healthcare systems). The best way of illustrating this point is to provide a contextual example that demonstrates the functionality of such a model. To this point, the following is a possible method of using the network diagram to facilitate the creation of useful and strategic policy regarding patient data.

If an organization was looking to maximize patient privacy (fundamental objective) as a way to ensure the privacy of patients whose data is being held by healthcare systems, labeled as O_1, one input could be to minimize sharing of patient data (means objective) labeled as m_5. However, m5 also relates to things such as minimize non-essential access to data (m_2) and ensure confidential collection of patient data (m_1). This type of model (Figure 4) illustrates a decision pathway that is therefore useful in helping an organization in achieving one or all of the fundamental objectives. Additionally, it provides different decision pathways for organizations to achieve the fundamental objective, which then allows the organization to choose pathways that complement their strengths. For this reason, based on the preferred value proposition, a number can then be assigned to the vector m instantiating the total summated value of any given decision pathway. Therefore, a common value model will take the form shown in Eq. (1) (Keeney 1992; Akkermans and Van Helden 2002) where k_i is the weight ascribed to the objective O_i and v_i is the relative desirability scaling:

$$v = \left(m_{1,} m_{2,\ldots,} m_n\right) = \sum_{i=1}^{n} k_i v_i(m_i) \qquad (1)$$

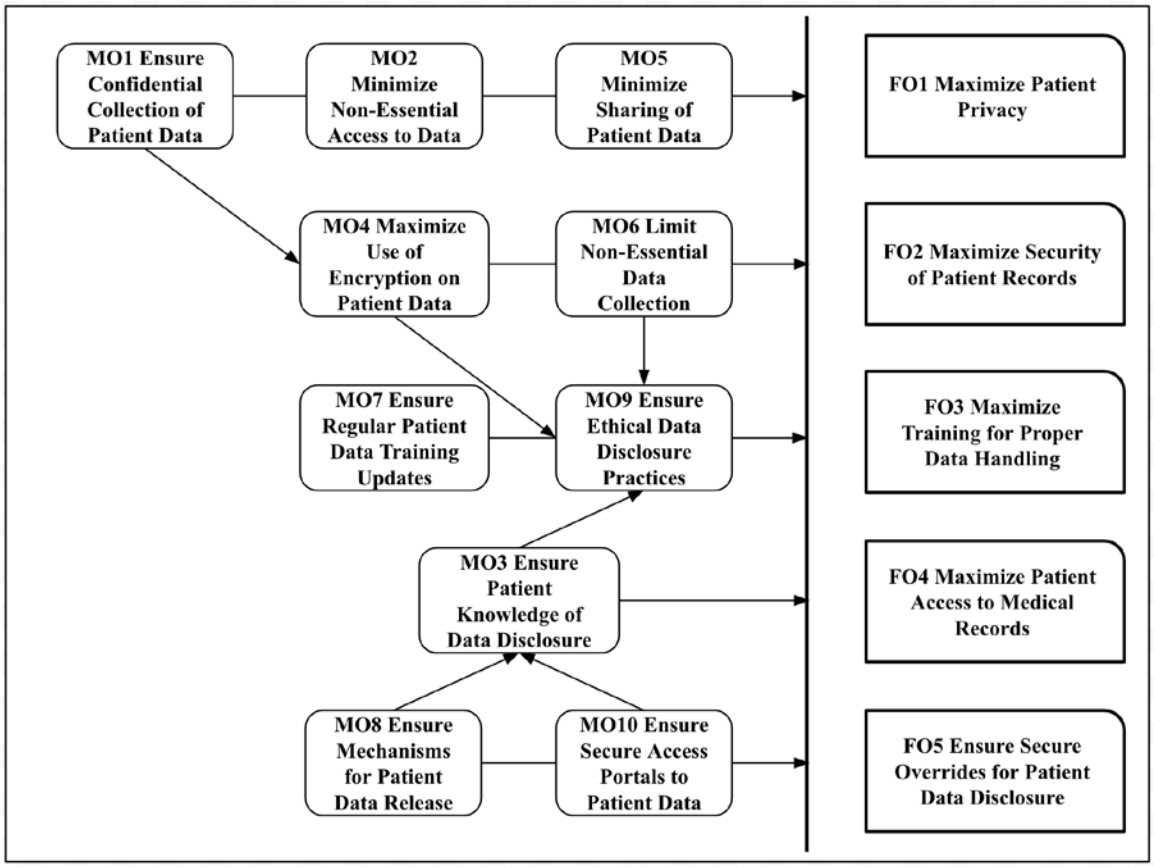

Figure 5. Means-end Network Diagram

Phase 2: The Public Value Forum

In the second phase of this research, the Public Value Forum or PVF (Keeney 1990) begins with the selection of participants to take part in the study. Utilizing the Fundamental Objectives developed in phase 1, the PVF will be useful in guiding the government's decision-making process related to the development of public policy around the use of patient data within healthcare organization systems in order to incorporate a patient-centric perspective. Once participants have been selected, the process of moving through each of the 5 steps of the PVF begins with step 1 (See Figure

3). The following is a recap of the general structure of the value forum (Keeney et al. 1990):

1. The policy problem is introduced and participants motivated
2. Objectives and attributes are defined and clarified
3. Ranking and Single-attribute utility functions elicited from all participants
4. Tradeoffs among the attributes are elicited from all participants
5. Construction of a Multi-Attribute Utility Models from results of all participants

Sample Selection

Prior to beginning the value forum, non-expert participants (N=40) were selected as a random sample of volunteers and split into 2 separate Public Value Forums of 20 participants each. Participants were solicited from the local area in places such as medical clinics and private doctors offices, with every 10^{th} person being asked to participate in the study. All were asked a serious of questions, ensuring they were legally able and willing to participate in the study and that no personally identifiable information would be retained by the researcher. The participants in each group ranged in age from 18 to 65 and had a split of a few more women than men. Participants had varying levels of educational background, and some participants had previous experience or education in the area of healthcare in the US. All of the participants had prior experience using US based healthcare, being mostly US-born citizens; however, several participants were non-US born citizens. The group was representative of the demographics of any major

metropolitan city of the mid-Atlantic region in the US. All participants were at least aware of the data collection practices of healthcare systems in the US prior to beginning the public value forum. Additionally, a sample of experts (N=5) was selected as a point of comparison to the non-expert participants.

As the purpose of this study is to determine patient-centric public values regarding ensuring the privacy and security of patient data in healthcare systems, an expert panel was not necessary (it can be said all persons are experts of their own values); however, it was intended to offer a point of comparison between general persons of the public and people in position to make decisions and with a more extensive background on the subject matter. Each expert has at least 5 or more years of experience in a decision making capacity (setting company policy, analyzing or using patient data in a decision-making capacity at an organization etc.), they currently directly influence organizational security policy, have at least 5 years of experience in US based healthcare and possess a greater awareness of the threats to patient data than general public knowledge.

Conducting the Public Value Forum

After participants are selected, step 1 of the Public Value Forum begins as they are presented the five fundamental objectives created in phase 1, with re-clarified defining attributes and problem context to ensure proper understanding of the decision context they are being asked to evaluate. After step 1 is complete, using these 5 fundamental objectives, ‘good’ and ‘bad’ scenarios are created along with four alternate scenarios.

These scenarios represent different instantiations of the five objectives based on the understanding of 'good' and 'bad' in the decision context for step 2. Once this is complete, a diagram (see Figure 6) representing the five objectives with their attributes, a 'value quote', and sub-objectives is developed and provided to the participants for reference during the remainder of the value forum. After the participants are satisfied with their understanding of the fundamental objectives created by phase 1 and placed in the form of a value tree for clarification and purposes of reference, the forum can then be moved to step 3 in the process.

After step 2 of the value forum was completed, participants are given the task of providing objective ranking and weighting, both prior to reviewing the varying implementation scenarios and again at the end of the study. The participants are asked to rank the five objectives for ensuring the privacy and security of patient data in healthcare systems (See Table 5); first in order of their perceived importance (1 = Highest, 5 = Lowest), then they are asked to review the 'good' and 'bad' scenario for each objective and rank the magnitude of change or 'swing' between these scenarios for each objective from largest (1) to smallest (5). This means participants assigned a weight that indicated the relative magnitude of a given 'swing' with respect to the scenario they rated as having the largest degree of change between the 'good' and 'bad' scenario. Next, the objective rated 1 is assigned a weight of 100, the lowest rating of 5 is given a weight of 0, and all others receive weight between 0-100 in decreasing increments by order of rank (Keeney 1990; Kirkwood, 1997). The purpose of the initial and final ranking and weighting was to determine how, if at all, the perceptions of participants change during the study from their

initial impression. Initially, they are only provided operational definitions of the objectives for ensuring the privacy and security of patient data in healthcare systems, but by the end of the study they have thoroughly examined a multitude of scenarios that express the potential applications of these objectives in real-world scenarios (Keeney 1990; Kirkwood 1997).

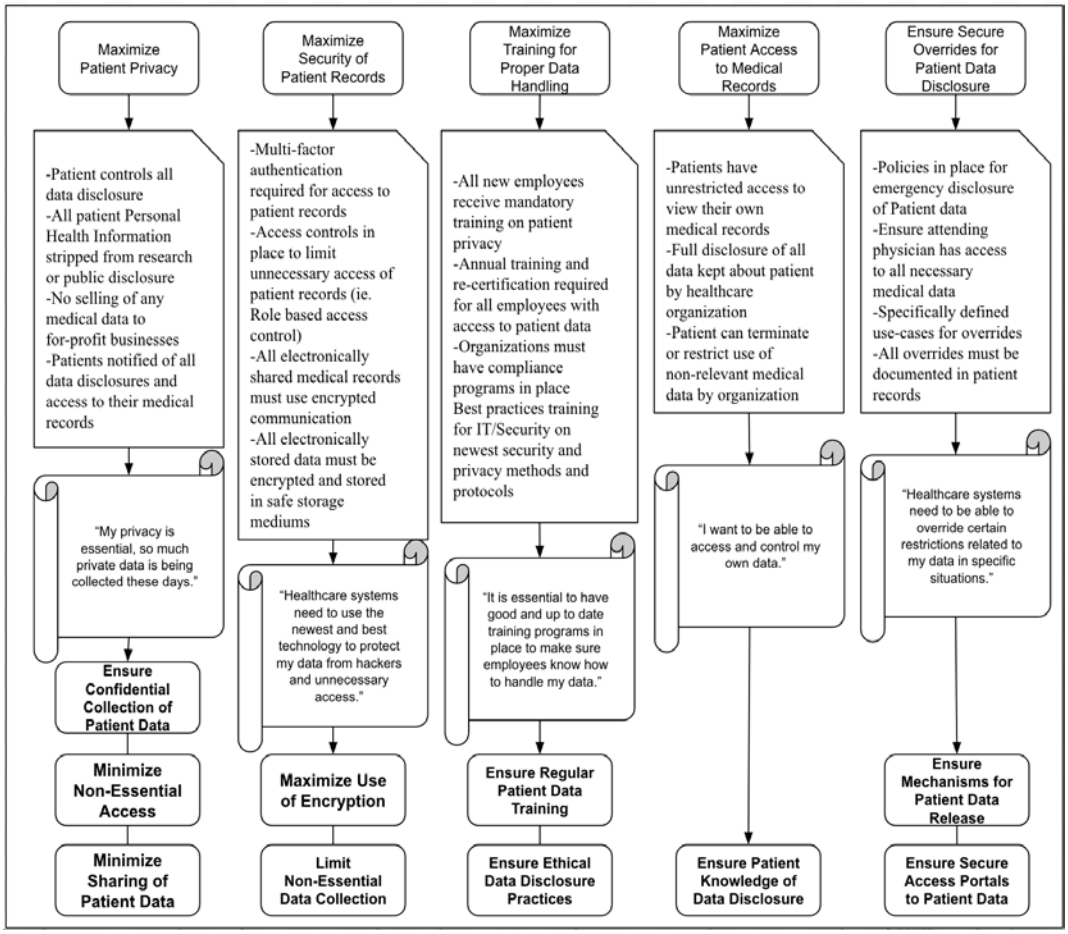

Figure 6. Value Tree Provided to Study Participants

Objective Importance Swing % (0-100)	Objective Importance Swing Rank (1-5)	Objective Importance Rank (1-5)	Fundamental Objectives
90	2	1	Maximize Patient Privacy
80	3	2	Maximize Security of Patient Records
100	1	3	Maximize Training for Proper Data Handling
0	5	5	Maximize Patient Access to Medical Records
60	4	4	Ensure Secure Overrides for Patient Data Disclosure

Table 5. Example of Objective Ranking and Weighting

In addition to the ranking and weighting of the objectives, participants also examined scenarios labeled A, B, C and D which expressed different potential real-world instantiations of ensuring the privacy and security of patient data in healthcare systems. These scenarios (see Figure 7) were juxtaposed with the 'good' and 'bad' scenarios and participants were asked to rank them in order of preference with respect to the 'good' and 'bad' scenarios, with their most preferred scenario receiving a 2 and least preferred receiving a 5. The 'good' scenario was rated as 1 and bad as 6 in order to provide a conceptual basis of comprehension in providing scenario preference ranks by the participants. After the ranking of the four scenarios, participants were asked to give an importance weight (Keeney 1990; Kirkwood 1997), again with respect to the 'good' and 'bad' scenarios, which were assigned 100 and 0 respectively. This was done to allow participants to demonstrate how close they felt the respective scenarios came to the concept of 'good' and 'bad' in these instantiations of the objectives beyond mere ranking (i.e. while a scenario may have ranked 2, a participant may have felt it was only 50% of

the way to being a ‘good’ implementation of the objectives, so this allowed them to demonstrate how ‘close’ to good they felt a scenario came). Once this task of ranking the various scenarios was completed, participants were then asked to rank each instance of the scenarios A, B, C and D by the individual objective.

During the evaluation of the overall scenarios, participants may have been forced to select an overall scenario ranking based on only a few aspects of a given scenario which they assigned more importance to than one or more other parts (i.e. participants may have ranked scenario C as the most overall preferred but only felt one objective C scenario was most preferable). In order to determine if participants may have actually preferred a differing implementation of each objective by scenario, they were asked to rank each scenario individually by the objective (see Figure 8). This allowed participants to, for example, select scenario C for the objective *Maximize Patient Privacy* as their most preferred while also being able to select scenario A for the objective *Maximize Security of Patient Records* as their most preferred. Participants were also asked to assign an importance weight to each ranking, using the same scale as before, with respect to how close to a ‘good’ implementation each scenario was represented. The purpose of this redundancy demonstrated the strength of preference for each individual scenario to each participant and how relative to ‘good’ each scenario was as well. After the entire scenario ranking and weighting was accomplished, the participants were finally asked to re-rank and weight the overall objectives for ensuring the privacy and security of patient data in healthcare systems as previously stated.

Privacy and Security Fundamental Objectives	Good Scenario (All objectives met 100%)	Scenario A	Scenario B	Scenario C	Scenario D	Bad Scenario (No objectives met at all)
Maximize Patient Privacy	-Patient controls all data disclosure -All patient Personal Health Information stripped from research or public disclosure -No selling of any medical data to for-profit businesses to earn profit by healthcare organizations -Patients notified of all data disclosures and access to their medical records	Government Sets comprehensive Policy and Regulations. Compliance enforced through law via financial penalties	Government sets only basic laws and policys, then ensures Organizations comply only to those specific standards through ensforcement via financial penalties	Government and Organizations work together to develop policy and regulations. Government penalizes failures, but organizations ensure compliance via self-audits validated by government	Organizations set their own policy and regulations, government is not involved and no compliance is enforced via government	-Patient controls all data disclosure -All patient Personal Health Information stripped from research or public disclosure -No selling of any medical data to for-profit businesses to earn profit by healthcare organizations -Patients notified of all data disclosures and access to their medical records
Scenario Rank (1-6)	1					6
Scenario % (0-100)	100					0

Figure 7. Holistic Scenario Ranking

Privacy and Security Fundamental Objectives

Scenarios	Maximize Patient Privacy	Rank (1-6)	Rank Importance Weight (0-100)	Maximize Security of Patient Records	Rank (1-6)	Rank Importance Weight (0-100)	Maximize Training for Proper Data Handling	Rank (1-6)	Rank Importance Weight (0-100)	Maximize Patient Access to Medical Records	Rank (1-6)	Rank Importance Weight (0-100)	Ensure Secure Overrides for Patient Data Disclosure	Rank (1-6)	Rank Importance Weight (0-100)
Good Scenario (All objectives met 100%)	-Patient controls all data disclosure -All patient Personal Health Information stripped from research or public disclosure -No selling of any medical data to for-profit businesses to earn profit by healthcare organizations -Patients notified of all data disclosures and access to their medical records	1	100	-Multi-factor authentication required for access to patient records -Access controls in place to limit unnecessary access of patient records (ie. Role based access control) -All electronically shared medical records must use encrypted communication -All electronically stored data must be encrypted and stored in safe storage mediums	1	100	-All new employees receive mandatory training on patient privacy -Annual training and recertification required for all employees with access to patient data -Organizations must have compliance programs in place -Best practices training for IT/Security on newest security and privacy methods and protocols	1	100	-Patients have unrestricted access to view their own medical records -Full disclosure of all data kept about patient by healthcare organization -Patient can terminate or restrict use of non-relevant medical data by organization	1	100	-Policies in place for emergency disclosure of Patient data -Ensure tending physician has access to all necessary medical data -Specifically defined usecases for overrides -all overrides must be documented in patient records	1	100
Scenario A	Government Sets comprehensive Policy and Regulations. Compliance enforced through law via financial penalties			Government Sets comprehensive Policy and Regulations. Compliance enforced through law via financial penalties			Government Sets comprehensive Policy and Regulations. Compliance enforced through law via financial penalties			Government Sets comprehensive Policy and Regulations. Compliance enforced through law via financial penalties			Government Sets comprehensive Policy and Regulations. Compliance enforced through law via financial penalties		

Figure 8. Individual Scenario Ranking

Results of the Public Value Forum

With the data collection from both non-expert and expert participants completed, an analysis was conducted on the findings for which the results will be discussed in the following five parts; Firstly, the overall initial and final Importance and Swing rankings and Swing weightings for both groups non-experts, notated as PVF1 and PVF2. Secondly, the overall scenario ranking and weightings for both groups of non-experts are detailed. Thirdly, the individual scenario ranking and weightings by objective are detailed. Fourthly, the expert results are then outlined in the same manner as the non-experts for comparative purposes and lastly the utility functions for non-experts, experts and overall will be demonstrated and discussed. In the following sections each Fundamental Objective will be notated as FO1, FO2, FO3, FO4 or FO5 corresponding to the numerical labels applied in phase 1 on this research (See Table 3) and the 3 groups are referred to as Public Value Forum 1 (PVF1), Public Value Forum 2 (PVF2) and Expert Value Forum (EVF). The entire process conducted in Phase 2 takes between 1 and 3 hours depending on the participants within the forum. Public Value Forum 1 took approximately 1.5 hours to conduct, while Public Value Forum 2 took 2 hours to perform. The expert Public Value Forum took slightly less time than both at just over 1 hour in length. Time spent by the researcher per phase will vary by the make-up on the participant groups.

PVF1 Initial Importance Rank, Swing rank and Swing weight Data for Non-Experts

To begin, each of the five objectives were defined for the participants of PVF1and they were asked to rank them in order of importance (See Table 5). The study found that in the initial rankings of the objectives, participants provided FO1 and FO2 with the highest overall median ranks of 1.5 and 2, while the objective FO3 was assigned a median rank of 3 and FO4 and FO5 were assigned median rankings of 4 and 5 respectively. Based on these initial rankings, participants, with only a definitional understanding of the objectives, clearly rate technical security measures and patient focused privacy protections as the highest areas of importance in this decision context.

Next, PVF1 participants assigned swing rankings for each objective based on the 'good' and 'bad' scenarios provided, which revealed that the difference between 'good' and 'bad' scenarios for each objective were likewise rated highest in the technical security and privacy driven objectives, with FO1 and FO2 each receiving a median swing rank of 2. Interestingly, it was found that participants also found FO3 as it relates to training persons to enact objectives such as FO1 and FO2, had a large change from 'bad' to good' and provided a median rank of 3, while FO4 and FO5 were given median ranks of 4. This seems to indicate that participants felt that not only were FO1 and FO2 very important overall, the swing between 'good' and 'bad' implementations was likewise of the greatest magnitude. With the weights (Keeney 1990; Kirkwood 1997) for each swing weight rating, participants were asked to demonstrate how drastic the change between 'good' and 'bad' scenarios was for each objective. This provided an astounding result that

demonstrated how important the objectives were as FO1 and FO2 received mean weights of 89.5 and 81.1 respectively (out of 100), while FO3 received 65.5, FO4 49.5 and FO5 a slightly lesser 42.75 mean weight. This would lead one to conclude that if faced with limited resources a strong focus on implementing strong technical security measures and focusing on improving patient-focused privacy measures might address the most pressing concerns of engaged users as these objectives were not only rated the highest, but also weighted most heavily by participants as having the largest degree of impact between a 'bad' and 'good' implementation.

Objective	**Mean of Importance Rank**	**Median of Importance Rank**	**Mean of Swing Weights**	**Median of Swing Weights**	**Mean Rank of Swing Weights**	**Median Rank of Swing Weights**
FO1	1.65	1.5	89.5	90	1.85	2
FO2	1.9	2	81.1	90	2.35	2
FO3	2.75	3	65.5	80	3.15	3
FO4	4.25	4	49.5	70	3.75	4
FO5	4.45	5	42.75	50	3.9	4

Table 6. PVF1 Initial Objective Ranks and Weights

PVF2 Initial Importance Rank, Swing rank and Swing weight Data for Non-Experts

After PVF1 was completed, a second Public Value Forum using another group of participants (PVF2, n=20) was conducted for validation and comparative purposes. Similar to PVF1, each of the five objectives were defined for the participants of PVF2 and they were asked to rank them in order of importance (See Table 6). The study found that in the initial rankings of the objectives, participants provided FO1 and FO2 with the highest overall median ranks of 1 and 3, while the objectives FO3, FO4 and FO5 were assigned median rankings of 4. Based on these initial rankings, participants in PVF2 held similar perceptions of importance to those in PVF1; however, PVF2 clearly felt the importance of objectives FO3, FO4 and FO5 was much harder to distinguish between than those of PVF1.

Next, PVF2 participants assigned swing rankings for each objective based on the 'good' and 'bad' scenarios provided, which revealed the difference between 'good' and 'bad' scenarios for each objective. Similar to PVF1, rated highest were the technical security and privacy driven objectives with FO1 and FO2 each receiving a median swing rank of 2. It was also found that participants felt FO3 and FO4 had large changes from 'bad' to good' and provided a median rank of 4, while FO5 was given a median rank of 5. Again, this seems to indicate that participants of PVF1 and PVF2 both felt that not only were FO1 and FO2 very important overall, the swing between 'good' and 'bad' implementations was likewise of the greatest magnitude. With the weights (Keeney 1990; Kirkwood 1997) for each swing weight rating, PVF2 participants were asked to

demonstrate how drastic the change between ‘good’ and ‘bad’ scenarios was for each objective. This provided an interesting result that demonstrated how important the objectives were as FO1 and FO2 received mean weights of 73.5 and 80.25 respectively (out of 100), while FO3 received 49, FO4 55.5 and FO5 a very low 32.25 mean weight. This would lead one to make similar conclusions to those drawn from PVF1, yet it is important to note that participants varied more in this forum as to the impact and importance of training in impacting the overall decision context. A clear takeaway supported by both forums, is that participants clearly believed that direct patient controls over data disclosure (FO1) and technical security measures (FO2) would make a clear and direct impact in solving this problem.

Objective	**Mean of Importance Rank**	**Median of Importance Rank**	**Mean of Swing Weights**	**Median of Swing Weights**	**Mean Rank of Swing Weights**	**Median Rank of Swing Weights**
FO1	1.75	1	73.5	85	2.25	2
FO2	2.6	3	80.25	87.5	2	2
FO3	3.55	4	49	50	3.4	4
FO4	3.4	4	55.5	62.5	3.45	4
FO5	3.7	4	32.25	0	3.9	5

Table 7. PVF2 Initial Objective Ranks and Weights

PVF1 Final Importance Rank, Swing rank and Swing weight Data for Non-Experts

After the overall and individual scenario ranking and weighting was completed, participants in PVF1 were then asked to re-evaluate their prior objective ranking and weightings to determine whether their perceptions changed based on the potential real-world implementations of the objectives (See Table 7). It was found that the overall importance rankings stayed relatively similar, with FO1 and FO2 flipping in rankings yet retaining median rankings above 2. FO5 rose in its median ranking to 4 from 5, while FO3 and FO4 stayed the same with a median ranking of 3 and 4 respectively. Swing rankings for each objective changed very little as it appears that seeing proposed instances of implementation did little to influence PVF1 participants understanding of the objectives, with rankings remaining the same and weights staying relatively similar to the initial figures.

Objective	Mean of Importance Rank	Median of Importance Rank	Mean of Swing Weights	Median of Swing Weights	Mean Rank of Swing Weights	Median Rank of Swing Weights
FO1	2.25	2	86.9	90	1.85	2
FO2	1.55	1	87	95	2	2
FO3	2.9	3	67.25	80	3.2	3
FO4	4.1	4	44.25	50	4	4
FO5	4.2	4	43.75	50	3.95	4

Table 8. PVF1 Final Objective Ranks and Weights

PVF2 Final Importance Rank, Swing rank and Swing weight Data for Non-Experts

Similar to PVF1, after the overall and individual scenario ranking and weighting was completed, PVF2 participants were then asked to re-evaluate their prior objective ranking and weightings to determine whether their perceptions had changed after seeing potential real-world implementations of the objectives (See Table 8). It was found that the overall importance rankings experienced a greater degree of delineation than in the initial rankings, with FO1 and FO2 having median rankings of 2; however FO3 and FO4 rose in its median rankings to 3 from 4, while FO5 stayed the same with a median ranking of 4. Swing rankings for each objective changed the most dramatically as it appears that seeing

proposed instances of implementation enhanced PVF2 participants understanding of the objectives. Median swing ranks for FO1 and FO2 remained at 2, while FO3 moved up from 4 to 3, FO4 stayed at 4 and FO5 fell from 4 to 5. While the magnitude of these changes appears relatively minor, FO3 initially had a mean weight of 49, while on the final evaluation the mean weight rose to 52.75. Alternatively, the fall of FO5 from 4 to 5 in swing rank did not result in such a large change (32.25 to 39 mean weight), indicating that the Value Forum process provided greater clarity and understanding to participants of PVF2.

Objective	**Mean of Importance Rank**	**Median of Importance Rank**	**Mean of Swing Weights**	**Median of Swing Weights**	**Mean Rank of Swing Weights**	**Median Rank of Swing Weights**
FO1	2.4	2	79	87.5	2.15	2
FO2	2.3	2	81.4	90	2	2
FO3	3.25	3	52.75	60	3.25	3
FO4	3.35	3.5	56	67.5	3.6	4
FO5	3.7	4	29	0	4	5

Table 9. PVF2 Final Objective Ranks and Weights

This final recap of Importance Rank, Swing Rank and Swing Weight is useful because it re-emphasizes the importance of the technical and procedural objectives (FO1 and FO2) as well as highlights the impact 'good' and 'bad' implementations of each objective has in the public perception of the privacy and security of their data in healthcare systems. Further, a deeper understanding of FO3 revealed that when participants were provided with real-world examples of scenarios illustrating the objectives, the training of persons charged with handling data received more importance and the difference between 'good' and 'bad' scenarios was viewed as much greater than initially perceived to be. This finding revealed the importance of both creating a comprehensive understanding of the concept of privacy and security in this context as well as how real-world instantiations of each objective can impact the public's perceptions of an objective's importance with respect to 'good' and 'bad' implementations.

PVF1 Scenario Selection Preference for Non-Experts

If government is looking to protect the privacy and security of data in healthcare systems from a patient-centric perspective, understanding the importance of the objective to their users is useful in directing the allocation of finite time and resources. It is also of equal importance to understand the means by which a government organization can enact those objectives to accomplish such a task, anticipating the preferred method by which users will respond to those measures in the most positive way. This was first done in the study by having participants evaluate the proposed implementation scenario 'options' in a holistic manner where the scenarios, labeled A, B, C and D, ranged from high

government involvement (scenario A) to very little/no government involvement (scenario D). Participants were asked to rank, based on their preference, the order in which the scenarios represented ‘good’ to ‘bad’ options, with 2 being their most preferred and 5 being their least preferred overall scenario for the objective’s implementation. Lastly, participants weighted their rankings relative to how ‘good’ or ‘bad’ they were compared to the baseline good and bad scenarios.

The results from this portion of the study (see Table 9) provided insight into public preferences with respect to the actions a government body should take in ensuring the privacy and security of data in healthcare systems from a patient-centric perspective. The study found that PVF1 participants tended to favor scenario C with a median rank of 3, mean rank of 2.95 and a mean weight of 74.5, demonstrating that they found an option where government and healthcare systems cooperate and work together with government only penalizing failures that result in actual damage to the patient is preferred in order to ensure the adequacy of these protection methods. By contrast, scenario D was the least preferred of all the scenarios receiving a median rank of 5 and a mean weight of 52.65, indicating that PVF1 participants did not find a ‘hands off’ government approach appealing. This approach leaves the vast majority of the responsibility and accountability for protecting data in the hands of the organization, with little reason for ensuring their own compliance. This contrast is very important for government organizations as it demonstrates that users clearly want mechanisms in place that work to ensure their data is safe, but they prefer to let healthcare systems have a higher degree of input in how such protections should be implemented and take place. This is an important takeaway for

healthcare systems as it appears to indicate PVF1 participants held a large degree of trust in these systems to do the right thing, without the constant threat and compulsion for government mandated compliance.

Scenario	Mean Rank	Median Rank	Mean Weight	Median Weight
A	3.15	3	73.55	80
B	3.35	3	68.75	77.5
C	2.95	3	74.5	80
D	4.55	5	52.65	60
Good	1	1	100	100
Bad	6	6	0	0

Table 10. PVF1 Scenario Selection Preferences

PVF2 Scenario Selection Preference for Non-Experts

For PVF2, the scenario selection process was conducted the same as in PVF1 with the results from this portion of the study (see Table 10) providing additional insight into public preferences in this decision context. The study found that PVF2 participants, much like PVF1, favored scenario C with a median rank of 2.5 and a mean weight of 76.05.

Also similar, scenario D was the least preferred of all the scenarios receiving a median rank of 5 and a mean weight of 35.5, indicating that PVF2 participants did not find a 'hands off' approach appealing. This approach leaves the vast majority of the responsibility for prevention in the hands of the user. While there are important similarities between PVF1 and PVF2, it must be noted that PVF2 clearly had stronger preferences between the 4 presented scenarios. Another interesting point is that both PVF1 and PVF2 preferred scenario C the most, a highly cooperative approach, and scenario A second most, a highly government directed approach. Future research may look to explore why a more moderate approach such as scenario B was not more preferred than scenario A as current methods of policy implementation in this decision context are most similar to scenario B.

Scenario	Mean Rank	Median Rank	Mean Weight	Median Weight
A	2.95	3	67.85	72.5
B	3.55	4	58.05	60
C	2.7	2.5	76.05	80
D	4.8	5	37.5	35
Good	1	1	100	100
Bad	6	6	0	0

Table 11. PVF2 Scenario Selection Preferences

PVF1 Individual Scenario selection by Objective for Non-Experts

In this final portion of phase 2, PVF1 participants were asked to rank, in order of preference, each scenario by the objective. This was done to assess whether participants may prefer different methods of implementation based on the given objective. The results (see Table 11) from this method of individual scenario selection and preference indicate that generally scenario C is the preferred choice for objective implementation with scenario B leading scenario C in only 1 objective, FO5. The results of this section are still overall consistent with the holistic scenario selection for PVF1 as Scenario A, B and C

are all close in weight with scenario C generally holding a moderate edge in every objective except FO5.

	FO1		FO2		FO3		FO4		FO5	
Scenarios	Median Rank (1-6)	Mean Weight (0-100)	Median Rank (1-6)	Mean Weight (0-100)	Median Rank (1-6)	Mean Weight (0-100)	Median Rank (1-6)	Mean Weight (0-100)	Median Rank (1-6)	Mean Weight (0-100)
Good Scenario	1	100	1	100	1	100	1	100	1	100
Scenario A	3	73.8	4	71.3	3	74.75	3	69.35	3	71.75
Scenario B	3	72.75	3	72.25	4	64.75	4	70.25	3	73.25
Scenario C	3	77	3	77	3	77	3	74.25	3.5	72.25
Scenario D	5	54.15	5	53.45	4.5	56.75	4	62.4	5	58.2
Bad Scenario	6	0	6	0	6	0	6	0	6	0

Table 12. PVF1 Individual Scenario Selection

PVF2 Individual Scenario selection by Objective for Non-Experts

Just as with PVF1 in this final portion of phase 2, PVF2 participants were asked to rank in order of preference, each scenario by the objective. This was done to assess whether PVF2 participants may prefer different methods of implementation based on the given objective. The results (see Table 12) from this method of individual scenario selection and preference strongly indicate that scenario C is the preferred choice for objective implementation with scenario A leading scenario B as the second choice in every objective. The results of this section are overall consistent with the holistic scenario selection for PVF2 as weights for Scenario A, B and C are all evenly distributed with scenario C holding a commanding edge for every objective.

	FO1		FO2		FO3		FO4		FO5	
Scenarios	Median Rank (1-6)	Mean Weight (0-100)	Median Rank (1-6)	Mean Weight (0-100)	Median Rank (1-6)	Mean Weight (0-100)	Median Rank (1-6)	Mean Weight (0-100)	Median Rank (1-6)	Mean Weight (0-100)
Good Scenario	1	100	1	100	1	100	1	100	1	100
Scenario A	3	69.1	3	66.6	3	61.1	4	61.85	3	63.85
Scenario B	3.5	68	4	55.5	4	52	4	56.25	3.5	53.5
Scenario C	3	75.5	3	76.25	2.5	68	3	73.5	3	69.75
Scenario D	5	48.7	5	50.5	4.5	50	4.5	53.75	4	51.05
Bad Scenario	6	0	6	0	6	0	6	0	6	0

Table 13. PVF2 Individual Scenario Selection

Expert Value Forum Results

Initial Importance Rank, Swing rank and Swing weight Data for Experts

As with the non-expert PVF1 and PVF2 participants, the value forum began by having each of the five objectives defined for the expert participants, and then having the participants rank the objectives in order of importance (See Table 13). The study found that in the initial rankings of the objectives, expert participants provided FO1 and FO2 with the highest overall median ranks of 2 and 1 respectively, while the objective FO3 was assigned a median rank of 3 and FO4 and FO5 were assigned median rankings of 4 and 5. Based on these initial rankings, experts, much like the non-expert participants, clearly rate technical and procedural patient privacy protection measures highest in importance in this decision context.

Next, expert participants assigned swing ratings for each objective based on the 'good' and 'bad' scenarios provided. This revealed that the difference between 'good' and 'bad' scenarios for each objective were different than in terms of importance with FO2 and FO3 being given swing ranks of 1 and 2. This indicates that while experts feel FO1 is important, more so than FO3, in terms of implementation effectiveness they felt that FO2 and FO3 were tied together and therefore FO3 rose in rankings. Much like the non-expert participants, experts felt FO4 and FO5 were both less critical in this decision context and both ranked and weighted them lower.

Objective	**Mean of Importance Rank**	**Median of Importance Rank**	**Mean of Swing Weights**	**Median of Swing Weights**	**Mean Rank of Swing Weights**	**Median Rank of Swing Weights**
FO1	2.6	2	69.6	89	3	3
FO2	1.2	1	98	100	1.2	1
FO3	3.2	3	87.4	89	2.2	2
FO4	3.8	4	19	0	4.6	5
FO5	4.2	5	52	60	4	4

Table 14. Expert Initial Ranks and Weights

Final Importance Rank, Swing rank and Swing weight Data for Experts

After the overall and individual scenario ranking and weighting was completed, expert participants were then asked to re-evaluate their prior objective ranking and weightings to determine whether, after seeing potential real-world implementations of the objectives, their perceptions had changed (See Table 14). It was found that the overall ranks and weights for every objective stayed nearly the same, with the swing weights for FO1 rising slightly from 69.6 to 74.6 and FO4 falling slightly from 19 to 16. The most interesting insight from this comparison between the expert initial and final rankings is both the consistency between them, and how the results compare to the non-experts. FO2 and FO3 are highly rated in all forums, yet non-experts gave FO1 a much higher rating across the board, perhaps due to the greater power yielded to the patients with respect to their control over data.

Objective	Mean of Importance Rank	Median of Importance Rank	Mean of Swing Weights	Median of Swing Weights	Mean Rank of Swing Weights	Median Rank of Swing Weights
FO1	2.6	2	74.6	89	2.8	3
FO2	1.2	1	98	100	1.2	1
FO3	3.2	3	87.4	89	2.2	2
FO4	3.8	4	16	0	4.8	5
FO5	4.2	5	52	60	4	4

Table 15. Expert Final Ranks and Weight

Scenario Selection Preference for Experts

In the same way non-expert participants were asked to evaluate scenarios, expert participants first evaluated the scenario 'options' in a holistic manner where the scenarios, labeled A, B, C and D, ranged from high organization involvement (scenario A) to very little organization involvement (scenario D). The experts were asked to rank, based on their preference, the order in which the scenarios represented 'good' to 'bad' options, with 2 being their most preferred and 5 being their least preferred overall scenario for the objective's implementation. Lastly, the experts weighted their rankings relative to how 'good' or 'bad' they were compared to the baseline good and bad scenarios.

The results from this portion of the study (see Table 15) provided insight into expert preferences with respect to the actions a government body or organization should take in ensuring the privacy and security of patient data in healthcare systems. The study found that the expert participants tended to favor scenario B and C with a median rank of 3 each and mean weights of 72.6 and 70.8 respectively, demonstrating that they found options similar to what is already being done (scenario B) or an option that gave the organization more control (scenario C) likely to be most effective. However, upon further discussion with expert participants, those who selected scenario B as most preferable indicated they did so because they knew the results based on the effectiveness of current policy being implemented in this way. Experts who selected scenario B as most preferable also selected scenario C as a second choice, noting they felt more flexibility by organizations would be more effective than more stringent government policy. Conversely, experts who selected scenario C as most preferable also selected scenario B as the second most preferable for similar reasons.

By contrast, scenario D was the least preferred of all the scenarios, receiving a median rank of 5 and a mean weight of 20.4. Experts also found Scenario A to be of little appeal with a rank of 4 and mean weight of 55.8. Experts' low rating for Scenario A and D could mean that while they disapprove of a heavy handed government approach, a near hands-off approach is even less appealing. This contrast is very important for governments implementing policy as it demonstrates that users, expert and non-expert alike, clearly want policy-based mechanisms in place that work to ensure their privacy and security,

but they prefer organizations maintain a higher level of control and discretion over the exact use and implementation of those mechanisms as opposed to having mechanisms forced upon them irrespective of relevancy to ~~a~~ healthcare systems' circumstances. It is important to note that the mean rank of Scenario C was 3 and the mean rank of B was 2.6, hence the swing weights accurately reflect scaling of the participants selection and demonstrate how close Scenario C and B were amongst experts in terms of strength of preference.

Scenario	Mean Rank	Median Rank	Mean Weight	Median Weight
A	3.4	4	55.8	40
B	2.6	3	72.6	70
C	3	3	70.8	80
D	5	5	20.4	15
Good	1	1	100	100
Bad	6	6	0	0

Table 16. Expert Scenario Selection Preferences

Individual Scenario selection by Objective for Experts

In this final portion of the study, expert participants were asked to rank, in order of preference, each scenario by the objective. This was done to assess whether participants may prefer different methods of implementation based on the given objective. The results (see Table 16) from this method of individual scenario selection and preference indicate that the experts, irrespective of the objective being addressed by the scenario, tended to prefer Scenario B. Again of note, Scenario C had a similar median rank and very close mean weight. Unlike the non-expert participants, experts placed more weight on Scenario B as a primary preference; meaning while Scenario C and B are the most preferred individual scenario implementations for experts and non-experts overall, scenario B is highest for experts and scenario C for non-experts. However, when discussing their choices with the experts, most maintained that the choice of scenario B over C was primarily attributed to a lack of motivation for challenging the status quo and a clear understanding of what is already in place rather than what could potentially be with another style of implementation.

	FO1		*FO2*		*FO3*		*FO4*		*FO5*	
Scenarios	**Median Rank (1-6)**	**Mean Weight (0-100)**	**Median Rank (1-6)**	**Mean Weight (0-100)**	**Median Rank (1-6)**	**Mean Weight (0-100)**	**Median Rank (1-6)**	**Mean Weight (0-100)**	**Median Rank (1-6)**	**Mean Weight (0-100)**
Good Scenario	1	100	1	100	1	100	1	100	1	100
Scenario A	4	57.2	4	56.2	4	56.2	4	54.8	4	54.8
Scenario B	3	72.6	3	72.6	3	72.6	3	72.6	3	72.6
Scenario C	3	69	3	69	3	70	3	71.4	3	71.4
Scenario D	5	20.4	5	20.4	5	20.4	5	20.4	5	20.4
Bad Scenario	6	0	6	0	6	0	6	0	6	0

Table 17. Expert Individual Scenario Selection Preferences

Public Value Forum Utility Function Results

In the final stage of phase 2, utility functions are calculated for each fundamental objective in the decision context for each of the 4 scenarios provided. This is done for the non-experts (both groups) and experts, and then using an overall utility for the combined groups it allows for a holistic model. This holistic model then enables the assessment of the efficacy of a policy derived from these alternatives. Therefore the importance of this calculation and subsequent model is twofold: Firstly, it allows an analysis of the scenario's utility within each objective to determine the preferences of each group as well as overall. Secondly, it enables a government organization or institution to build a policy which addresses each fundamental objective and measures its utility by scenario.

To calculate the group utilities, an individual utility was calculated for each participant in both the non-expert and expert groups. These were then weighted and summated (see formula pg. 31) to create an overall utility for each group. The scaled weight for each participant in each group was the same (1/n) as the study is interested in the overall values of the public regarding the decision context. Therefore, whether a participant is considered an "expert" or a "non-expert" on the subject matter should not give them any greater weight in the overall solution as they are all equal members of the general public. The purpose of having multiple groups was to analyze if there were any significant differences in values that may warrant a different weighting scale and for overall comparative purposes. While differences do exist, the results tend to show similar trends amongst groups and overall preferences are generally similar. Additionally, the smaller

sample size of the expert group (n=5) is more susceptible to expressions of significant differences in rank and weight between participants.

The utilities for each objective (see table 17), which are expressed by scenario, demonstrate the same trends observed in the previous sections results. Clear preference for Scenario B and C exist for experts and non-experts alike; however, experts tend to prefer Scenario B and non-experts express greater preference for Scenario C. These preferences are reflected by the corresponding utilities for each group and are still generally seen in the final overall utilities when both groups' results are combined. It is important to note that in the non-expert group, a solution similar to Scenario A would receive a higher utility than B in 3 of the 5 objectives for PVF1 and PVF2; however, those differences are all marginal, typically within 0.1 points. Likewise, a solution addressing the expert group's concerns similar to Scenario B is preferred more than Scenario C in 4 out of 5 objectives, yet in FO4 scenario A is most preferred. It is also useful to note that the order of scenario preference maintains overall consistency between groups and by objective in overall utility, the only variation being FO5 for all 3 groups. This may suggest solutions that take an approach of moderation, ceding slightly more control to organizations in the application of these objectives, will be consistently more appealing to those most affected by their implementation.

The use of these utility calculations by a governmental institution will be in determining the overall efficacy of a policy aimed at maximizing the privacy and security of patient

data in healthcare systems. For example (see table 17), an organization may attempt to address the problem of privacy and security in their organization by working to specifically address the fundamental objectives FO1 and FO2 and giving minimal effort or resources to the remaining objectives. However, they only have the ability to implement policy, which addresses these concerns in a manner similar to Scenario C and the remaining objectives receive treatment similar to that of Scenario D. An organization would then calculate the overall utility of their policy by adding FO1 and FO2 scenario C utility of 19.7 and 20.8 and the remaining objectives scenario D utility, 9.6, 8.1 and 6.4 respectively. This would result in the policy having an overall scaled utility of 64.6 out of a possible 100. However, with current implementation closer to scenario B, it would also be possible to express a current utility score demonstrating the value of efforts using current methods of implementing policy. For example, by replacing all scores with those of scenario B and comparing them to scenario C, the overall utility of current implementation type B would be 65.8 compared to 74.2 for scenario C. Therefore, it would be possible to increase the overall utility related to policy implementation through organizational collaboration with a government institution that could allow for implementation of objectives using solutions similar to that of Scenario C.

	Maximize Patient Privacy			
	Non-Experts Utility VF1	Non-Experts Utility VF2	Experts Utility	Overall Utility
Scenario A	19.2	18.7	12.9	18.3
Scenario B	19.1	19.1	16	18.7
Scenario C	20.9	19.8	14.7	19.7
Scenario D	14.6	13.4	4.4	12.9
	Maximize Security of Patient Records			
	Non-Experts Utility VF1	Non-Experts Utility VF2	Experts Utility	Overall Utility
Scenario A	18.8	17.2	17.3	17.9
Scenario B	18.8	14.5	22.5	17.3
Scenario C	19.9	21.5	21.9	20.8
Scenario D	14.2	14	6.5	13.3
	Maximize Training for Proper Data Handling			
	Non-Experts Utility VF1	Non-Experts Utility VF2	Experts Utility	Overall Utility
Scenario A	16.1	12.3	14.8	14.3
Scenario B	12.9	10	19.3	12.3
Scenario C	15.4	12.1	18.7	14.3
Scenario D	12	8.3	5.3	9.6
	Maximize Patient Access to Medical Records			
	Non-Experts Utility VF1	Non-Experts Utility VF2	Experts Utility	Overall Utility
Scenario A	12.8	15.6	4.2	9.8
Scenario B	12.7	13.9	3.4	9.1
Scenario C	13.2	19.3	2.1	10.9
Scenario D	11.9	13.2	0	8.1
	Ensure Secure Overrides for Patient Data Disclosure			
	Non-Experts Utility VF1	Non-Experts Utility VF2	Experts Utility	Overall Utility
Scenario A	8.7	6	6.9	7.4
Scenario B	10.1	6.2	11.4	8.4
Scenario C	9.6	6.5	12.4	8.5
Scenario D	7.4	5.9	4.1	6.4

Table 18. Overall Public Value Forum Utility Function Results

Phase 3: Developing an Objective-based Decision Model

In order to improve the privacy and security of patient data stored by healthcare systems, a useful model which includes both the patient-centric concerns and governmental regulations could be used to analyze their current levels of protections with respect to the privacy and security of patient data. This patient-centric privacy and security assessment model should not simply identify whether objectives were done successfully, but the

degree of success (or lack of) in order to demonstrate areas in need of improvement. The model, and therefore the results of the analysis, can also serve as a means for comparing the privacy and security of patient data amongst various healthcare systems by the government, providing more than a basic pass/fail auditing mechanism and providing healthcare systems quantified metrics as a baseline for improvement. This is where Keeney's (1992; 1996) Value Focused Thinking (VFT) for decision analysis can help create an objective-based framework for government regulatory organizations, such as the National Office for Health Information Technology (HealthIT.gov), as well as healthcare systems to model the necessary objectives for maximizing the privacy and security of patient data and demonstrate gaps in their performance relative to their goals which can then be improved upon (Merrick et al. 2005a; Merrick et al. 2005b; Merrick & Garcia 2004).

This process occurs in five basic steps adapted from Keeney (1992) and Merrick et al. (2005a; 2005b) and can derive its objectives directly from literature which has previously established and defined the measurable regulatory objectives for privacy and security in healthcare (i.e. HIPAA and HITECH) as well as from the process outlined in phase 1 (see figure 2, pg. 23). Additionally, privacy and security experts in the realm of healthcare should be interviewed to elicit the necessary importance and swing weights to fully build out the proposed model and perform an analysis on a real use-case healthcare system. For this research, an example of how this can be done is provided as a proof-of-concept, using objectives derived from phase 1 (see table 3. Pg. 49) as well as directly from HIPAA and HITECH regulations. However, before this can be done, it is first necessary

to discuss in detail the steps which will be undertaken as the methodology for this research. It is important to note that this model will use fundamental objectives, which are defined by Keeney (1992; 1996) as "providing a structure for clarifying the values of interest in a given decision context and provide a basis for evaluating alternative," while strategic objectives are "relevant to a wide range of decision contexts, to a long time period, and to many levels in an organization." This proposed model must then use fundamental objectives for measuring the privacy and security of patient data in healthcare systems, but will organize them in the context of strategic objectives which meet the general goals of an organization implementing the privacy and security measure as directed by HIPAA and HITECH.

The process for developing and quantifying the privacy and security objectives will involve the following steps (Keeney 1992, 1996; Merrick et al. 2005):

(1) Critical analysis of the relevant literature, which is conducted by the analysts, to identify the factors that are fundamentally important for the organization's success in maximizing the privacy and security of patient data. The analyst ensures that important objectives are not omitted.

(2) The objectives are structured into a hierarchy that clarifies the differences between strategic and fundamental objectives and eliminates redundancies of objectives.

(3) Experts define attributes for the objectives to clarify exactly what the objectives mean and to measure any possible consequences. The measurements also include importance and swing weighting for each objective in the model by experts in the privacy and security of patient data in healthcare systems (Kirkwood 1997).

(4) Developing a utility function over the strategic objectives that indicates value trade-offs among the objectives. The utility function should reflect the viewpoints of privacy and security experts in an organizational context related to maximizing the privacy and security of patient data.

The best way to describe the utility of this type of value model is to consider the various fundamental objectives as being O_1, …O_n and m_1 as a measure for a fundamental objective O_1. Therefore, it follows that the vector m= (m_1, m_2, …, m_n) would provide a description of a particular path in which a fundamental objective is delivered. The accumulated value of m would then serve as a measure (quantitative or qualitative) of the characteristic resources and abilities that would fit the decision context (i.e. assessing the privacy and security of patient data in healthcare systems). In the additive case (Keeney 1992), the overall utility *v* for any alternative described by m_1-m_n is:

$$v = \left(m_1, m_{2,\ldots,} m_n\right) = \sum_{i=1}^{n} k_i v_i(m_i)$$

where n is the number of attributes, where k_i is the weight ascribed to the objective O_i and v_i is the relative desirability scaling.

(5) Assessing the value gaps of individual objectives based on the outcomes of the analysis. This identifies areas for improvement and allows a cost-benefit analysis to be performed to determine to most cost-effective areas to implement change and target finite organizational resources.

Through the completion of these steps a proposed proof-of-concept model will be developed to demonstrate its potential usefulness in the context of an organizational assessment. This is done through the analysis of a given healthcare organization's implementation of the fundamental objectives necessary to maximize the privacy and security of patient data in healthcare systems. The healthcare system used for this proof-of-concept test is based in the US mid-Atlantic area and is a large provider of patient care in the region. In phase 2, experts from this healthcare system provided weights and suggested measurements for the fundamental objectives, which can then be used as an example of how this model can be implemented by either healthcare systems or government agencies seeking to assess how well an organization is protecting patient data. The remainder of phase 3 explains how this proposed model can be used to assess of overall privacy and security of patient data in healthcare systems as a proof-of-concept and how it can be fully implemented in later research.

The goal of phase 3 is that experts can utilize the proposed model to evaluate each of the objective criteria on their respective measurement scales individually and the totality of the assessment will provide a summated score of how well a healthcare organization protects patient data. The completed score will be scaled in order to create a comparative rating between 0 and 100 (0 being the worst and 100 the best) to indicate the relative success of any given healthcare system in addressing the objectives for maximizing the privacy and security of patient data. A gap analysis of each objective and strategic context can also be completed to demonstrate which objectives were most completely addressed by the healthcare system and which ones have room for improvement. This analysis demonstrates both the impact of the objective itself (its given contribution to the model), the degree to which it was addressed by the healthcare system, and the gap or "degree" for potential improvement. Additionally, with this information a cost-benefit analysis could be used determine which objectives with the highest gaps in performance should be rectified first, comparing the cost to improve by the scaled improvement in their overall scoring metric. This cost-benefit analysis should be based on the objective's weighted impact to the overall model and the cost of implementing such an improvement to the healthcare system. This is important as a healthcare system may identify several areas to target improvement, but some may require costs which are untenable to the organization. Instead, objectives elucidated by the model which are the most impactful and cost effective to address should be those focused on first with the model providing quantitative evidence for doing so.

Identifying and Structuring Objectives

In this section, an objective hierarchy for measuring privacy and security protections related to patient data in healthcare systems is developed from the existing literature (ie. HIPAA and HITECH) as well as from the research conducted in phase 1 in order to incorporate a patient-centric perspective. Here, each fundamental objective is categorized by strategic objective, which are general in nature and applicable across a wide range of healthcare system types. This is done to maximize the readability of the model and aggregate categorically similar objectives for assessment purposes. Additionally, it allows a more granular gap analysis allowing a comparison amongst various categories, multiple category objectives or objectives within a single category. The objective-based hierarchy (Figure 9 & 10) represents the culmination of fundamental objectives which can be used to measure the efficacy of a healthcare system's privacy and security measure related to protecting patient data and identify gaps for future improvement. Further, as experts from the aforementioned healthcare system in phase 2 facilitated definitions for measurement scales, as well as importance and swing weights, an example of a potential use case to demonstrate proof-of-concept is provided with the text to illustrate the model development process. To fully develop this hierarchy, each category was developed by the experts using the *Guide to Privacy and Security of Electronic Health Information* as provided by The Office of the National Coordinator for Health Information Technology, available from HealthIT.gov. This guide helped to ground the hierarchy and its relevant categories and objectives firmly in the necessary US Regulatory framework and incorporate the patient-centric objectives in an easy to manage way.

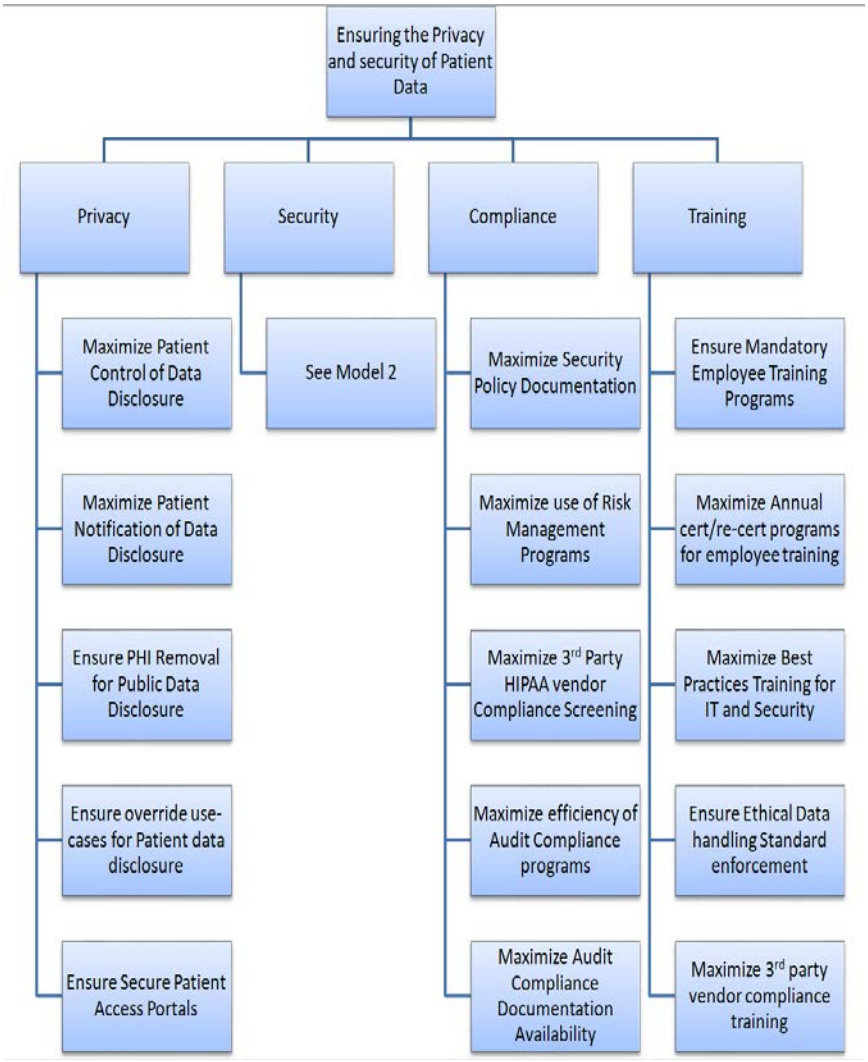

Figure 9. Objective Framework Model pt.1

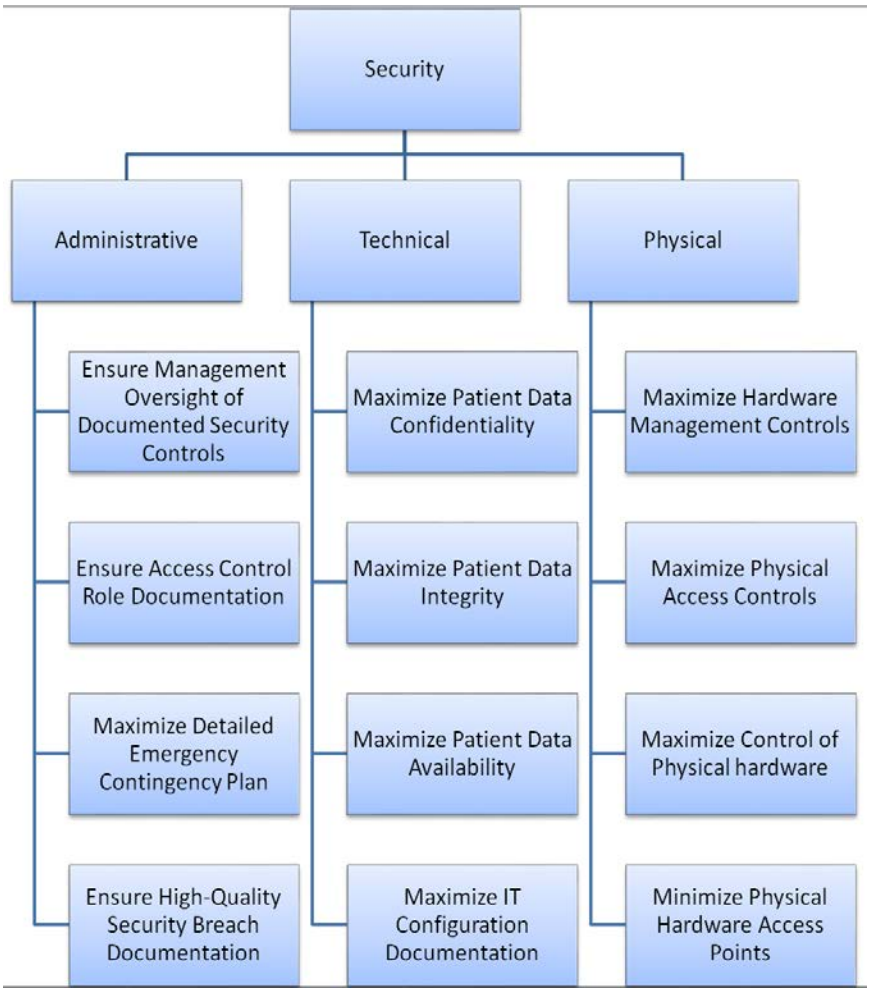

Figure 10. Objective Framework Model pt.2

Defining Measurable Objective Ranges

In this phase, experts refine the attributes for the objectives to clarify exactly what the objectives mean and to determine if any additional objectives of importance should be added. Additionally, experts determine the criteria used to measure these objectives in order to ensure a consistent model with which the various objectives can be evaluated by a government agency or healthcare system. This process can generally take several hours if all expert participants meeting at one time and in a single location. However, repeated

meetings over a period of several days may be necessary if some participants are unable to attend a single session for a prolonged period of time. All experts were able to meet and define each objective in a single session lasting 2 hours, defining and clarifying each objective one at a time and determining effect measurement scales for each one by a simple majority decision, guided by the researcher.

Therefore, the output of this phase (example, see Table 19) in the development of the evaluation model requires the following: all necessary objectives for evaluation, consistent definitions to ensure uniform understanding of the objectives, and scales by which the objectives can be measured by the model. Some evaluation measures will require constructed scales as not all objectives may have easily quantifiable metrics by which they can be measured; however, they are still important to the decision context and should be included. The exact definitions are set through the collective efforts of the expert participants and structured by the researcher to ensure they remain properly contextualized for the problem at-hand.

Objective	Definition/Measure	Scale
Maximize Patient Data Confidentiality	All Patient Data, both PHI and non-PHI is encrypted while at rest and in transit using the latest security protocols. System is up-to-date (within 15 day update cycle) with latest security updates. Ideal score is 5, each 3 day interval beyond 15 results in 1 rank deduction, unencrypted PHI data is 2 rank deduction and non-PHI data is 1 rank deduction.	#1 to 5. 5 Ideal 4 Above Adequate 3 Adequate 2 Substandard 1 Failing

Table 19. Example Objective Definition and Measurement Scale

Defining Attribute Weights and Developing the Value Function

Once the measurements scales and definitions are completed, importance and swing weighting for each objective in the model is elicited from the healthcare privacy and security experts (Kirkwood 1997). In order to do this, importance scales are constructed for each objective based on the proposed measurement scale. The importance weights are from 0 to 100 with 0 being the worst and 100 being the best. The experts weight points on the measurement scale with the importance weight, which allows for the construction of single-attribute value functions (Figure 11) (Keeney 1992, 1996; Merrick et al. 2005). Importance weights are intended to demonstrate an actual measure of difference between, for example, a rank of 1 and a rank of 5 for an objective. The goal is that if a 5 rating is the best and weighted 100 then a 4, which is weighted as a 75, is essentially 75% as good.

This distinction is important, because without importance weights we are unable to discern how much worse a 4 is to a 5 as perceived by the rater of a given objective.

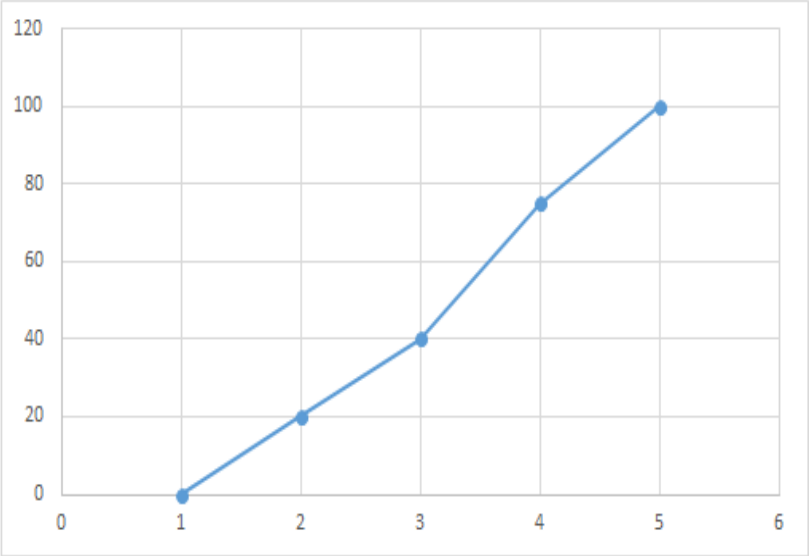

Figure 11. Example of Single-Attribute Utility for Maximize Patient Data Confidentiality

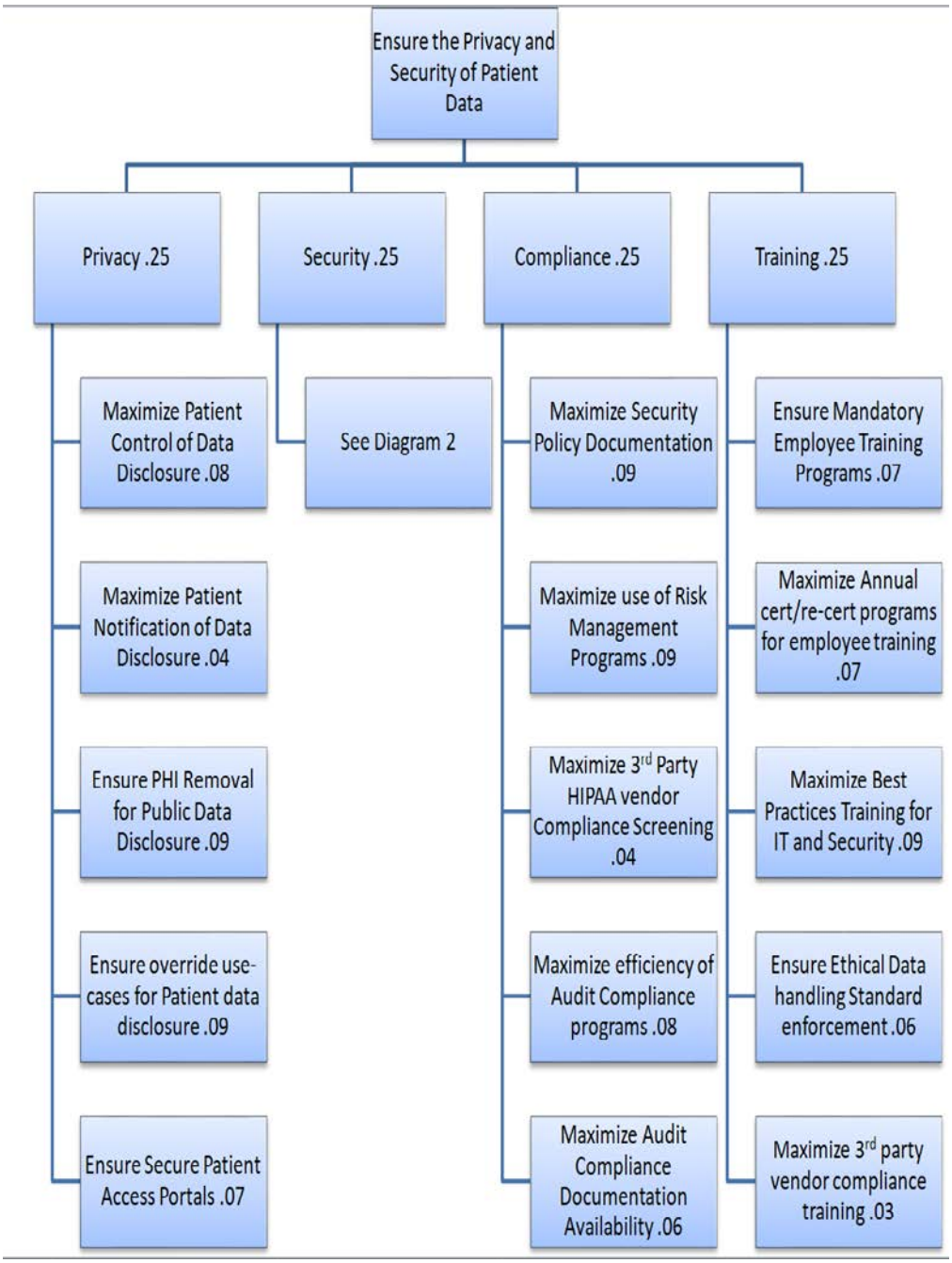

Figure 12. Weights for Objective Framework Model pt. 1

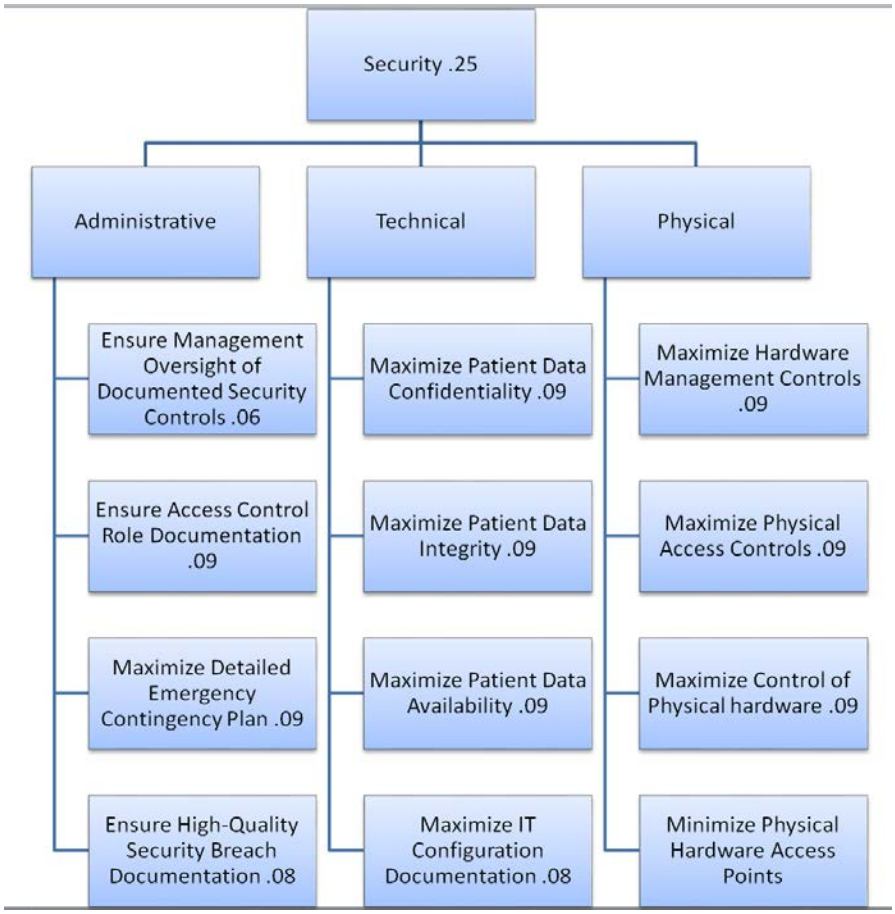

Figure 13. Weights for Objective Framework pt. 2

After importance weights have been assigned swing weights are elicited for each objective relative to the others as well as by category (Figure 12 & 13). This allows the framework to create a holistic evaluation (multi-attribute value function) of a healthcare system's protection of patient data and define the overall impact of each objective relative to an organization's strategic goals (See Figure 14). This will further allow an organization to perform a gap analysis by objective and category in order to develop processes to improve the privacy and security of patient data within their organization. The solution uses scaled weights (Kirkwood 1997) to derive global weights for the

objectives themselves as well as for the strategic objectives. Similar to importance weights, we need a metric to define the impact of an objective in the overall context of the decision. Participants should be asked to review ‘all good’ and ‘all bad’ scenarios for each objective and rank the magnitude of change or ‘swing’ between these scenarios for each objective from largest to smallest by strategic category (each category has its objectives ranked separately). This means participants are then asked to assign a weight that indicates the relative magnitude of a given ‘swing’ with respect to the scenario they rated as having the largest degree of change between the ‘good’ and ‘bad’ scenario. To do this the objective that ‘swings’ the most in each category should be given a swing of 100 and each rank given a lower number going as low as 0, relative to the one above it in the ranking. The objective weights are then scaled by taking each weight and dividing it by the total of all weights. Global weights, which are necessary for categorical comparisons, are created by weighting each category and then scaling those weights and multiplying each objective’s scaled weight by their respective category’s scaled weight.

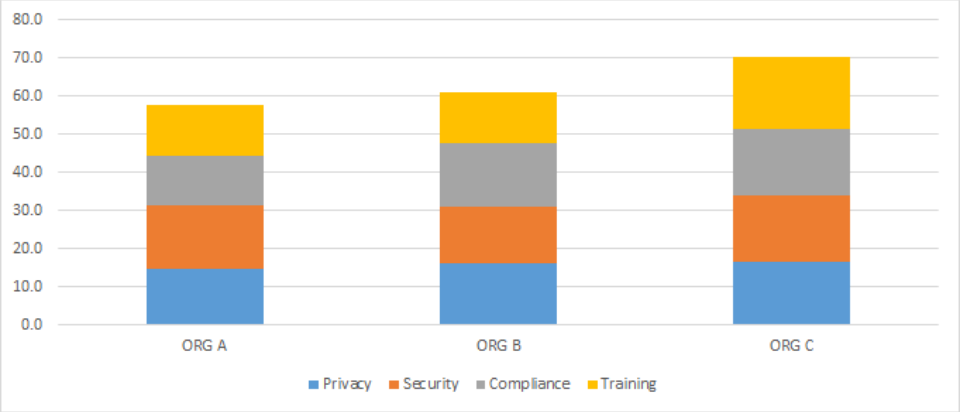

Figure 14. Categorical Breakdown of Overall Utility Score

Objective Value Gap Analysis

By scaling the weights to provide a global weighting, this allows organizations to perform a gap analysis (Figure 14) by objective and category in order to develop process improvements to overcome any deficiencies in evaluation of their organizations privacy and security protections of patient data (Merrick et al. 2005). This is based on the objective's single-attribute utility function and can be measured at the categorical level or in a more granular fashion at the objective level. If the developed functions demonstrate a maximum allowed utility of 28, but the proposed solution only provides 16.5, then a gap is demonstrated. However, this gap may be relatively small and fail to have a value proposition for correcting this deficiency, while another with a gap of 14 out of a maximum of 26, could be an ideal candidate for reviewing for possible process improvements to rectify this gap. This would require a detailed cost-benefit analysis of that particular organization to determine the cost for reducing each value gap detailed in the value gap analysis.

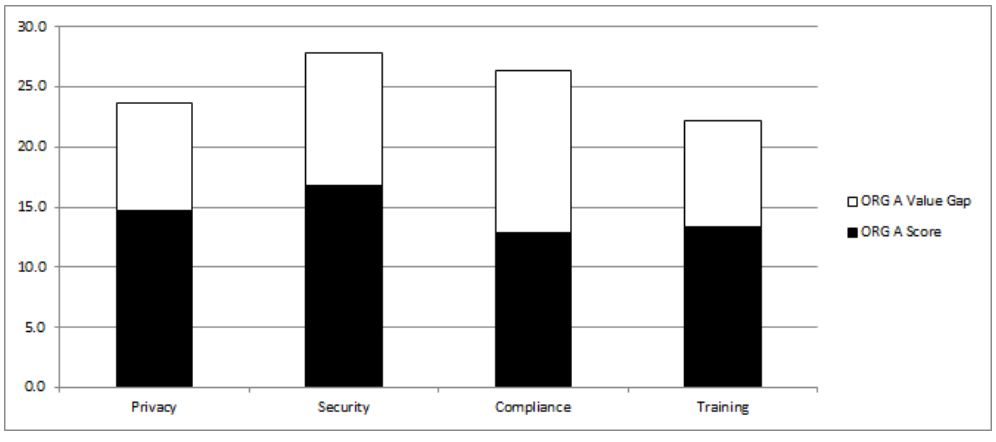

Figure 15. Example of Categorical Value Gap Comparison

Hence, this is an important part for the evaluation of the protections afforded to patient data in a particular healthcare system. It demonstrates to an organization both where a solution is lacking and, if more than one area requires improvement, which is the most impactful. This enables an organization to more prudently address areas of need with the highest value per dollar, as it is unlikely unless the organization has limitless resources, that all objectives will be adequately addressed and therefore produce no value gaps to improve upon. Additionally, a sensitivity analysis can be performed to test how much the value gaps change with variations in these weights (Merrick et al. 2005a), as different organizations and experts may suggest assigning differing weights to various objectives. For that reason, it is important to understand how value gaps can change based on differences in weights in order to ensure the gap analysis is robust to any possible changes in the model's objective weights.

Discussion

Each phase of the research provides unique theoretical, methodological and practical contributions to the field of information systems in the context of healthcare. In the following subsections the contributions from each phase will be discussed individually and then any limitations related to this work will be detailed. Lastly, a discussion of possible future directions for academic research based on these findings will take place. To begin, the contributions for phase 1 will be detailed as each phase builds on the contributions of the last.

Phase 1 Discussion

Based on this research there are three distinct, yet loosely named, categories into which the findings fall: cultural, procedural and technical. For the purpose of this research, the following understandings of each category are considered to discern between the three. The cultural category is intended to convey the understanding that objectives in this category address patient privacy and security concerns through cultural mechanisms such as the inculcation of proper data handling procedures and ethical standards of conduct by members of the organization. These objectives are intended to be socialized into the organization as expectations of behavior through means such as compliance and/or training programs to raise awareness, in order that the organization has expected standards of etiquette that go beyond simply adhering to the rules to avoid punishment.

Unlike the cultural category, the procedural category is intended to be understood as the composition of rules, regulations, guidelines and legal consequences intended to enforce compliance to proper standards of legal conduct within the organization. These are intended to act as strict guidelines to which members of such an organization must adhere or risk direct penalty for failing to do so.

The technical category is intended to deal specifically with the technological aspect of protecting the privacy and security of patient data and can encompass aspects of the procedural and cultural category, but it is intended to apply to objectives that are directly tied to technology and its use and implementation by organizations. The norms of distribution and appropriateness elicited during interviews with respondents resulted in

value-driven objectives that specifically address these societal norms using mechanisms in one of these categories based on the provided meaning of each.

For example, the fundamental objective "*Maximize Patient Privacy (FO1)"* was developed using Value-focused Thinking and to express a norm of distribution using contextual integrity as a theoretical framework. Respondents were clearly expressing a desire to control the dissemination of information based on an implicit minimum expectation of privacy when sharing relevant medical information with their healthcare provider. The attributes that make up this fundamental objective include having direct control over their data's disclosure and patient notification of any disclosure of their records. Based on our interviews, this fundamental objective expresses the desires of our respondents to have clear procedural expectations for ensuring the proper use of data exchange mechanisms like electronic medical records and non-medical staff access to data.

Another fundamental objective that fits in this category is *"Ensure Secure Overrides for Patient Data Disclosure (FO5),"* which describes the desire of those interviewed to enact specific use-cases by which the healthcare system can override patient control and disclosure rules and gain access to their data. While *FO1* can be seen as a means of empowering the patient to take an active role and responsibility for protecting one's own data, *FO5* is intended to allow members of an organization to engage in routine behavior that is universally acceptable according to the implicit societal norms by making them explicit social expectations for the disclosure of patient data. Based on the respondent's

interviews within this study, which probed these norms for greater understanding, it is suggested that this might be accomplished by developing healthcare applications for smartphones that allow patients easier methods for taking an active role in the use of their data. This could include things like what type of information should and should not be shared and when sensitive information is shared by an individual, the implied responsibility of maintaining the integrity of that interaction by not re-sharing without explicit consent.

Another fundamental objective, "*Maximize Training for Proper Data Handling (FO3)"* falls into the cultural category. When discussing this category, it is important to note that this objective was developed to mean that respondents felt that certain societal norms should be inculcated into the cultural fabric of the organization, such as ethical standards of behavior or ensuring the organization always seeks to implement the newest and best security techniques. This fundamental objective is illustrative of norms of appropriateness, where society looks to ensure user information will be handled properly by organizations such that only what is necessary may be revealed and highly sensitive information will remain confidential. Respondents clearly indicated that certain norms were of such importance that an organization should strive to educate employees to comply with them as an innate behavior. The reason for this is that our respondents viewed organizations as part of the social system with a responsibility for enabling society to enact and enforce their societal norms, such as ethical standards of conduct, within the workforce. Today we can see this reflected in corporate social responsibility movements and initiatives by both society and organizations; however, the impetus

behind this fundamental objective is to ensure mechanisms exist to enforce compliance to explicit cultural standards of conduct.

The last category into which our objectives fit is that of the technical, comprised of the fundamental objectives, *"Maximize Security of Patient Records (FO2)"* and *"Maximize Patient Access to Medical Records (FO4)."* Both of these fundamental objectives represent norms of distribution as they seek to enable patients to safeguard their information by ensuring technical mechanisms are in place to do so. For example, respondents indicated they wanted the ability to control data disclosure as well as the ability to remove non-relevant data from their records. While healthcare systems may be hesitant to implement some of these types of features, providing patients with some level of control over their data would go a long way based on the responses given by participants in this study. Additionally, while patients may not have extensive expertise in technical methods of security, many are acutely aware of things such as multi-factor authentication, role-based access controls and encryption. As such, they have the expectation that organizations will always remain on the cutting-edge of such technology, believing that the price for such security is never too high. As a society there is an implicit normative expectation among our respondents that technology should ensure privacy, and that security of their personal information is maintained at all times. Therefore, we developed these objectives based on the societal norms concerning norms of distribution that reflected this implicit belief in order to ensure the prevention of violations of contextual integrity due to lapses in the security of patient data.

These three categories help to demonstrate the unique attributes of the five fundamental objectives as they relate to norms of distribution and appropriateness based on the theoretical framework of contextual integrity. They are representative of societal norms surrounding the flow of information in the context of patient data in healthcare and were operationalized using Value-focused Thinking. This operationalization allows us to create actionable objectives that governments and organizations can use to address patient-centric concerns related to the privacy and security of their data in healthcare systems and facilitate the creation of mechanisms to address them.

Phase 2 Discussion

Based on the results of the phase 2 analysis, three distinct conclusions can be drawn which further the academic literature. The first conclusion is that baseline regulations must exist in order to aid organizations in the protecting the privacy and security of patient data and provide users with the confidence that the issue is being addressed. The second is that users desire strong up-to-date technical security controls in place that healthcare systems should use to protect their information from potential theft or improper disclosure. Finally, non-expert participants far preferred a scenario C style implementation of the fundamental objectives, which calls for more cooperation amongst government institutions and healthcare systems to implement these privacy and security protections and less top-down government regulation than the scenario B style that exists today. This is different from the expert participants who felt that the current scenario B style of addressing privacy and security was best, yet as a second choice also picked

scenario C as the next best means of protecting patient data. This includes findings that deepen the understanding of patient-centric privacy and security concerns, while reinforcing our current knowledge on the topic. Additionally, it demonstrates that the value forum methodology is capable of accurately reproducing results across numerous random samples of culturally similar non-experts. This is to say that the Public Value Forum, using fundamental objectives developed using contextual integrity as a normative framework, accurately portrays cultural attitudes related to the privacy and security of patient data among random samples of similar populations. Therefore, this is an advantage of this study as the two public value forums conducted provided similar conclusions and serve to validate the reliability of the findings based on them. Also, using an expert-only value forum provided unique insights into the differences between what can be considered substantive experts as compared to non-experts in the field of healthcare as it relates to patient privacy and security. These differences serve to illuminate key areas for future research opportunities and the need for additional research in this area, as experts and non-experts show a clear disconnect in how (the objective implementation) they believe the privacy and security of patient data is best protected.

These three distinct conclusions provide a great deal of insight into the values of the general public regarding the protection of the privacy and security of patient data at an organizational and governmental level. The results of the public value forum demonstrate a clear desire by participants to have clear regulations, policies and procedures that elucidate required protections of all forms of patient data in healthcare systems. Scenario D that provided little or no governance to this issue, regardless of objective, was the least

preferred by virtually all non-expert and expert participants, as it received no top rankings and 30 last place rankings. Scenario A, requiring heavy governmental involvement, was least preferred by all expert participants and received no first place rankings. This showed that both experts and non-expert participants were wary of solutions, which involved either too much or too little government involvement. During interviews with participants in both the expert and non-expert forums, follow-up questions regarding this point showed that participants believed that it was too difficult for the government to "keep up" with the rapid advances in technology. Many believed that ceding more control over the way in which patient data is protected in the form of stricter government regulations would reduce healthcare systems' burdens. However, nearly all participants agreed that the government should still penalize failures by healthcare systems to protect patient data as a means of preventing abuses by said organizations should no entity exist to hold them accountable.

Participants also indicated the need for strong technical security controls by ranking *FO2 Maximize Security of Patient Records* highly in the objective ratings as well as through the selection of scenarios, indicating that a high degree of technical tools should be implemented by healthcare systems for protecting patient data. In the application of policy and technical controls, participants demonstrated clear preferences for more control over final implementation by healthcare systems rather than through more government oversight. With respect to enforcement, participants still believed that the government should enforce penalties for failures to ensure healthcare systems simply do not ignore their obligation to protect patient data. However, participants contextualized

failure as actual breaches in which data was compromised, rather than failure to comply with stated rules or regulations. This was interesting and, when probed about this distinction, most participants responded that government compliance audits would only direct healthcare systems to be compliant to the rules, which would not necessarily cause them to spend on protections that would actually increase data security. Essentially, participants felt that overly burdensome government involvement would only serve to distract healthcare systems from the goal of maximizing patient privacy and security. Instead, by working together, healthcare systems could meet basic government regulations, be held accountable for actual failures, and implement more effective measures for protection the privacy and security of patient data as it relates to their own unique situation.

At the holistic scenario level, Scenario C was the clear preference in the value forum for both non-expert forum groups but only the second choice for the expert forum, which was composed of individual instantiations of the five objectives and had the following characteristics: Government and healthcare systems work together to develop regulations and policy, government penalizes failures that compromise patient data, and healthcare systems perform self-audits which are reported to the government for validation and compliance purposes. This is important to note in the context of the overall user scenario selection as it can be said that even if something is 'good for you,' if it is forced upon a person or organization, it may be rejected regardless of the risk, or simply performed at the bare minimum requirement, for which there is some support in the literature for this assertion. As Herley (2009), in the context of security and usability noted, "users reject

advice since it offers to shield them from the direct costs of attacks, but burdens them with increased indirect costs, or externalities. Since the direct costs are generally small relative to the indirect ones they reject this bargain. Since victimization (i.e. breaches of patient data privacy and security) is rare, and imposes a one-time cost, while security advice applies to everyone and is an ongoing cost, the burden ends up being larger than that caused by the ill it addresses." Hence, having some regulation to enforce protocols and technical controls in place, but giving healthcare systems input in the policy and regulation development process proved popular even at the individual scenario ranking level. In contrast to both non-expert groups, the expert forum selected scenario B, an implementation style most similar to what is done now, as most preferable. When asked why this was the case, most expert participants indicated that, while they thought scenario C could represent a better way of doing things, scenario B was a "known quantity" and preferred not to alter how things were done. This was supported by the results of the expert forum in that scenario B was ranked highest, 2.6 mean rank and 72.6 mean weight, while scenario C was ranked second highest, 3 mean rank and 70.8 mean weight. This insight is very useful as non-expert participants ranked scenario A, a very government heavy approach as their second choice, 3.15 mean rank and 73.55 mean weight, and put scenario B at 3.35 and 68.75 respectively. This would suggest that non-expert participants feel that the current means of protecting the privacy and security of patient data are insufficient, which was also supported by follow-up questions, and that either scenario C or A would likely yield better results.

These points clearly support the three distinct conclusions drawn and mentioned previously in that they illustrate a very clear desire among the general public to have well defined laws, regulations, procedures, and technical controls developed cooperatively between healthcare systems and the government for the protection of the privacy and security of patient data. Hence it can be said that in order to solve a problem as complex as protecting patient data in healthcare systems, it is important to understand the interplay between the information itself and the decision-making framework employed by an individual or organization. Research, with respect to decision-making, has long recognized that no simple connection between ‘‘more information’’ and ‘‘better decisions’’ exists (Sarewitz et al., 2000; Sarewitz & Pielke 2007). For that reason, simply adding more information with the implication being a greater understanding of the decision context, cannot be said to either solve the problem or demonstrate the shortcomings of the decision maker (Sarewitz & Pielke 2007). There are several reasons why simply adding more information alone to the discussion may not improve decision outcomes or outright solve the problem, among them being; the information is not relevant to user needs; it is not appropriate for the decision context; it is not sufficiently reliable or trusted; it conflicts with users’ values or interests; it is unavailable at the time it would be useful; it is poorly communicated (Sarewitz & Pielke 2007). Further yet, those who stand to benefit or be adversely affected the most will have a greater stake in the outcome of such decisions (Sarewitz & Pielke 2007). This is highly relevant to the study in that the value forum methodology seeks to address several of these concerns, namely; relevance, appropriateness to decision context and perhaps most important of all, it seeks to involve the most affected stakeholders in the decision process.

Phase 3 Discussion

The results of phase 3 provide relevant practical implications to both government and organizational institutions as the multi-objective decision model was developed using both the patient-centric objectives from phase 1 as well as objectives developed directly from existing (i.e. HIPAA and HITECH) government regulations. The model provides government-based regulatory bodies the ability to assess the privacy and security of patient data at various healthcare systems, providing them the ability to rank and stratify these systems based on a quantitative metric. As the model is objective based, maximizing the privacy and security of patient data in healthcare systems, it presents several unique advantages over other methods for undertaking similar efforts. By creating a singular definition for measuring each objective and assigning proper weights to each one, using an objective-based hierarchy allows for easy comparison between an unlimited number of relevant options without modifying the model or inadvertently altering preference rating by evaluating a new healthcare system.

The model provides further practical uses as not only a means for comparing multiple healthcare organizations, but as a self-assessment tool within the healthcare system itself. This is due to the value gap assessments performed in step 5 of the phase 3 methodology, which enable healthcare systems to clearly see in which objectives they fall short and then target resources efficiently to address those shortcomings. By assessing the value gaps within an organization, they can then perform a cost-benefit analysis to determine

which gaps should be addressed to maximize their return on investment. This type of analysis acknowledges that it is unlikely that any firm has the likely unlimited resources necessary to address all of their potential value gaps. Therefore a quantitative metric by which the largest gaps are identified would enable each individual firm to then determine the objectives they should address with finite resources to maximize their benefit.

Limitations and Future Directions

As with most qualitative research, this study is subject to a basic limitation of its methodological approach. The process of identifying values from interview data is largely subjective and interpretive and while researchers may strive to maintain a professional distance, there is always a possibility that some personal biases may influence the results; however, being conscious of this during all three steps in phase 1 should help to reduce or eliminate this prospect. The previous basis for this research and the critical reflections of the interviewee's statements was useful in helping to show how these various interpretations emerged in the research (Klein & Myers 1999). For this reason, it is believed that being aware of the intellectual biases actually helped with being objective within the analysis of the data. Further, Walsham (1995) recognized this to be an issue when carrying out intensive research and in regard to the role of the researcher wrote; "the choice should be consciously made by the researcher dependent on the assessment of . . . merits and demerits in each particular case (p. 5)." It is the goal that in strictly following the value-focused thinking method, theoretically constrained by the use of contextual integrity, and being conscious that our interpretations should not serve to influence this research, it can provide confidence in the outcome of this study.

Based on the research presented in this paper, there are three broad categories which exist for future research opportunities. The first opportunity is that the list of objectives identified in this research can be subjected to psychometric analysis using separate large samples. This can help, for example, in developing a model for measuring the impact of protection measures on patient's perception of privacy and security in healthcare systems. A second opportunity exists for intensive research to be undertaken to establish relationships between particular fundamental and means objectives; however, while Keeney (1992) contends that fundamental and means objectives are related and implicit, logical relationships appear to exist between the fundamental and means objectives, specific relationships need to be researched. The final opportunity is such that further quantitative work should be carried out to assess how the subscales of means and fundamental objectives relate to each other. In the cybersecurity field, the topic of patient-centric privacy and security concerns is constrained by the absence of well-grounded concepts that are developed in a systematic theoretical and a methodologically sound manner as the topic itself is still a newer concept relating to the mass aggregation of patient data. The fundamental and means objectives that are presented in this paper make a contribution towards the development of theory specific to patient-centric privacy and security in healthcare systems, a largely overlooked IS research stream.

Conclusion

The information necessary in the context of decisions related to maximizing the privacy and security of patient data in healthcare systems can be said to be strongly influenced by highly complex and important factors such as: institutional structures, prior practice, political stakes and distributions of power (Sarewitz & Pielke 2007). These factors, found in all the affected stakeholders, influences to a high degree the types of information that decision makers will need and use in attempting to solve the problem of protecting patient data (Sarewitz & Pielke 2007). Therefore, this research incorporated both experts and non-experts in the research process to embed these important factors in the decision-making process of organizations and government institutions. This grounds the decisions based on this process firmly in the values and interests of the vested stakeholders (those most affected). Hence, academics who seek to understand the behavior of scientific information in complex decision contexts such as protecting patient data must converge on the recognition that the utility of such information depends on the dynamics of the decision context and its broader social setting (Jasanoff and Wynne, 1998; Pielke et al., 2000). This is to say, the presentation of knowledge for its own sake does not provide utility, and thus it is important to recognize that the contribution of this research is that it promotes knowledge by providing application utility to the decision maker.

Gibbons (1999) describes the conversion from the gold standard of ‘‘reliable knowledge,” self-determined by scientists, to ‘‘socially robust knowledge;” This socially robust knowledge, which is the goal of both phase 1 and phase 2, is intended to be three

important things: Firstly, it is "valid not only inside but also outside the laboratory. Secondly, this validity is achieved through involving an extended group of experts, including lay 'experts'. Thirdly, because 'society' has participated in its genesis, such knowledge is less likely to be contested than that which is merely reliable (1999, p. C82)." This is the crux upon which this research rests as it has sought to incorporate these dimensions of the decision making process in order to transform "reliable knowledge" into that of useful "socially robust knowledge" that can aid in maximizing the privacy and security of patient data in healthcare systems, demonstrated by the model presented in phase 3.

The research presented in this paper examines the relatively unexplored area of patient-centric privacy and security concerns related to patient data held by healthcare systems in the field of information systems. This investigation, mixing qualitative and quantitative methods, which used value-focused thinking, contextual integrity, the public value forum and multi-attribute utility modeling, revealed the objectives and scenarios which the general public find most important and provide the greatest perceived protections, which are essential for developing measures and protections for patient data at a policy level by governments and organizations. Therefore, this is a significant contribution as previous research in this area is under-developed and as such falls short of being able to direct the proposal and generation of tangible patient-centric measures and protections for patient data in healthcare systems. This research extends the process further and provides a multi-attribute utility that incorporates the values of experts and non-experts in order to

provide a flexible model for improving policy at a governmental and organizational level that maximizes policy value.

Lastly, this research provides a useful model, which can be used to evaluate and critique such protections related to the privacy and security of patient data in healthcare systems that uniquely incorporates the patient perspective. This allows both healthcare systems and government institutions to evaluate, measure and improve upon any shortcomings in their implementation of methods intended to protect the privacy and security of patient data within their organizations.

References

Akkermans, H. & Van Helden, K. 2002. Vicious and virtuous cycles in ERP implementation: a case study of interrelations between critical success factors, European Journal of Information Systems, 11 (1), pp. 35–46.

Algarni, A., Xu, Y., & Chan, T. 2017. An empirical study on the susceptibility to social engineering in social networking sites: the case of Facebook. *European Journal of Information Systems*, *26*(6), pp. 661-687.

Anderson, J. M. 2003. Why we need a new definition of information security. *Computers & Security*, *22* (4), pp. 308-313.

Anderson, B. B., Vance, A., Kirwan, C. B., Eargle, D., & Jenkins, J. L. 2016. How users perceive and respond to security messages: a NeuroIS research agenda and empirical study. *European Journal of Information Systems*, *25*(4), 364-390.

Angst, C. M., Agarwal, R., & Downing, J. 2006. An Empirical Examination of the Importance of Defining the PHR for Research and for Practice. *SSRN Electronic Journal*.

Angst, C. M., & Agarwal, R. 2009. Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS quarterly*, *33*(2), pp. 339-370.

Arndt, R. 2017, August 16. Many of the attacks in the U.S. come from tools bought on the darknet or illicit websites. Retrieved April 05, 2018, from http://www.modernhealthcare.com/article/20170816/NEWS/170819925

Atchinson, B. K., & Fox, D. M. 1997. The Politics of the Health Insurance Portability and Accountability Act. *Health Affairs, 16* (3), pp. 146-150.

Bansal, G., & Gefen, D. 2015. The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern. *European Journal of Information Systems*, *24* (6), pp. 624-644.

Bansal, G., Zahedi, F., & Gefen, D. 2010. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems*, *49* (2), pp. 138-150.

Barrows, R. C. & Clayton, P. D. 1996. Privacy, Confidentiality, and Electronic Medical Records, *Journal of the American Medical Informatics Association*, Volume 3, Issue 2, pp. 139–148.

Barth, A., A. Datta, J.C. Mitchell, & H. Nissenbaum. 2006. "Privacy and contextual integrity: Framework and applications," Proc. of IEEE Symposium on Security and

Privacy.

Baskerville, R. 1993. Information systems security design methods: implications for information systems development. *ACM Computing Surveys,25*(4), pp. 375-414.

Belanger, F., & Cossler, R. 2011. Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly,35*(4), pp. 1017-1041.

Belanger, F., & Xu, H. 2015. The role of information systems research in shaping the future of information privacy. *Information Systems Journal,25*(6), pp. 573-578.

Belton, V. 1986. A comparison of the analytic hierarchy process and a simple multi-attribute value function. European Journal of Operational Research, 26(1), pp. 7-21.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. 2015. What do users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly* 39 (4), pp. 837–864.

Bourgeois, F. C., Nigrin, D. J., & Harper, M. B. 2015. Preserving Patient Privacy and Confidentiality in the Era of Personal Health Records. *Pediatrics,135*(5).

Brisson, G. E., Neely, K. J., Tyler, P. D., & Barnard, C. 2015. Privacy versus confidentiality: more on the use of the electronic health record for learning. *Academic*

Medicine, *90*(8), 1001.

Burns, A. J., Johnson, M. E., & Honeyman, P. 2016. A brief chronology of medical device security. *Communications of the ACM*, *59* (10), pp. 66-72.

Burns, A. J., Posey, C., Courtney, J.F., Roberts, T.L. & Nanayakkara, P. 2017a. Organizational information security as a complex adaptive system: insights from three agent-based models. *Information Systems Frontiers* 19 (3), pp. 509–524.

Burns, A. J., Posey, C., Courtney, J.F., Roberts, T.L. & Nanayakkara, P. 2017b. Examining the influence of organisational insiders' psychological capital on information security threat and coping appraisals. *Computers in Human Behavior* 68 (March), pp. 190–209.

Campbell, B., Thomson, H., Slater, J., Coward, C., Wyatt, K. & Sweeney, K. 2007. 'Extracting information from hospital records: What patients think about consent', Quality and Safety in Healthcare, Vol. 16, No. 6. pp. 404–408.

Chen, P. Y., Kataria, G., & Krishnan, R. 2011. Correlated failures, diversification, and information security risk management. *MIS quarterly*, pp. 397-422.

Chen, Y., Ramamurthy, K., & Wen, K. W. 2012. Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems*, *29* (3), pp. 157-188.

Choi, B. C., Jiang, Z., Xiao, B., & Kim, S. S. 2015. Embarrassing exposures in online social networks: An integrated perspective of privacy invasion and relationship bonding. *Information Systems Research*, *26* (4), pp. 675-694.

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. 2017. Organizational information security policies: a review and research framework. *European Journal of Information Systems*, *26* (6), pp. 605-641.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. 2013. Future directions for behavioral information security research. *computers & security*, *32*, pp. 90-101.

Crossler, R. E., & Posey, C. 2017. Robbing Peter to pay Paul: Surrendering privacy for security's sake in an identity ecosystem. *Journal of the Association for Information Systems*, *18* (7), pp. 487.

Culnan, M. & Williams, C. 2009. "How Ethics Can Enhance Organizational Privacy: Lessons from the ChoicePoint and TJX Data Breaches," MIS Quarterly (33:4), pp. 673-687.

Culnan, M.J. 1993. "How Did They Get My Name?," An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use," MIS Quarterly, pp. 341-363.

Culnan, M.J. & Armstrong, P.K. 1999. "Information Privacy Concerns, Procedural Fairness and Impersonal Trust: An Empirical Investigation," Organization Science (10:1), pp. 104-115.

D'Arcy, J., Hovav, A., & Galletta, D. 2009. User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20* (1), pp. 79-98.

Davis, J. .2017, August 21. Los Angeles provider breached by ransomware attack, over 260,000 patients affected (UPDATED). Retrieved April 05, 2018, from http://www.healthcareitnews.com/news/los-angeles-provider-breached-ransomware-attack-over-260000-patients-affected-updated

Dhillon, G., & Backhouse, J. 2001. Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal, 11* (2), pp. 127-153.

Dhillon, G., Oliveira, T., Susarapu, S., & Caldeira, M. 2016. Deciding between information security and usability: Developing value based objectives. *Computers in Human Behavior, 61*, pp. 656-666.

Dhillon, G. & Smith, K. J. (2017), "Defining Objectives for Preventing Cyberstalking", *Journal of Business Ethics,* Vol. 145, No. 1, pp. 1-22.

Dhillon, G., & Torkzadeh, G. 2006. Value-focused assessment of information system security in organizations. *Information Systems Journal, 16* (3), pp. 293-314.

Dhillon, G., Challa, C., & Smith, K. 2016. Defining Objectives for Preventing Cyberstalking. *ICT Systems Security and Privacy Protection IFIP Advances in Information and Communication Technology,* pp. 76-87.

Dinev, T., Xu, H., Smith, J. H., & Hart, P. 2013. Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems, 22* (3), pp. 295-316.

Dyer, J. S. 1990. Remarks on the analytic hierarchy process. *Management science, 36*(3), pp. 249-258.

French, A. M., Guo, C., & Shim, J. P. 2014. Current Status, Issues, and Future of Bring Your Own Device (BYOD). *CAIS, 35*, pp. 10.

Fundamentals of the Legal Health Record and Designated Record Set. (n.d.). Retrieved July 13, 2017, from http://library.ahima.org/doc?oid=104008

Garba, A. B., Armarego, J., Murray, D., & Kenworthy, W. 2015. Review of the information security and privacy challenges in Bring Your Own Device (BYOD) environments. *Journal of Information privacy and security*, *11*(1), pp. 38-54.

Gerlach, J., Widjaja, T., & Buxmann, P. 2015. Handle with care: How online social network providers' privacy policies impact users' information sharing behavior. *The Journal of Strategic Information Systems*, *24*(1), pp. 33-43.

Gibbons, M., 1999. Science's new social contract with society. Nature 402, C81–C84 (Supplemental).

Goel, S., Williams, K., & Dincelli, E. 2017. Got phished? Internet security and human vulnerability. *Journal of the Association for Information Systems*, *18*(1), pp. 22.

Gordon, W. J., Fairhall, A., & Landman, A. 2017. Threats to Information Security — Public Health Implications. *New England Journal of Medicine*,*377*(8), pp. 707-709.

Greenaway, K. E., Chan, Y. E., & Crossler, R. E. 2015. Company information privacy orientation: a conceptual framework. *Information Systems Journal*, *25* (6), pp. 579-606.

Gregory, R., & Keeney, R. L. 1994. Creating Policy Alternatives Using Stakeholder Values. *Management Science, 40* (8), pp. 1035-1048.

Herath, T., & Rao, H. R. 2009a. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), pp. 154-165.

Herath, T., & Rao, H. R. 2009b. Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), pp. 106-125.

Herley, C. 2009. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 workshop on New security paradigms workshop* (pp. 133-144). ACM.

Hevner, V. A. R., March, S. T., Park, J., & Ram, S. 2004. Design science in information systems research. MIS quarterly, 28(1), pp. 75-105.

Hsu, J. S. C., Shih, S. P., Hung, Y. W., & Lowry, P. B. 2015. The role of extra-role behaviors and social controls in information security policy effectiveness. *Information Systems Research*, *26*(2), 282-300.

Hunter, M.G. 1997. The use of RepGrids to gather data about information systems analysts. Information Systems Journal, 7, pp. 67–81.

Hu, Q., Xu, Z., Dinev, T., & Ling, H. 2011. Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM*, *54* (6), pp. 54-60.

Hui, K. L., Teo, H. H., & Lee, S. Y. T. 2007. The value of privacy assurance: an exploratory field experiment. *MIS Quarterly*, pp. 19-33.

Jasanoff, S. & Wynne, B. 1998. Science and decision-making. In: Rayner, S., Malone, E.L. (Eds.), Human Choice and Climate Change. Battelle Press, Columbus, pp. 1–88.

Johnson, M. E., & Willey, N. 2011. Will HITECH heal patient data hemorrhages? In Proceedings of the 44th Hawaii International Conference on Systems Sciences, pp. 1-10.

Johnston, A. C., & Warkentin, M. 2010. Fear appeals and information security behaviors: an empirical study. *MIS quarterly*, pp. 549-566.

Johnston, A. C., Warkentin, M., McBride, M., & Carter, L. 2016. Dispositional and situational factors: influences on information security policy violations. *European Journal of Information Systems*, *25* (3), pp. 231-251.

Kamoun, F., & Nicho, M. 2014. Human and organizational factors of healthcare data breaches: The Swiss cheese model of data breach causation and prevention. *International Journal of Healthcare Information Systems and Informatics (IJHISI)*, *9*(1), pp. 42-60.

Karjalainen, M., & Siponen, M. 2011. Toward a new meta-theory for designing information systems (IS) security training approaches. *Journal of the Association for Information Systems*, *12*(8), pp. 518.

Keeney, R. L. & Raiffa, H. 1976. Decisions with Multiple Objectives: Preferences and Value Tradeoffs, Wiley, New York.

Keeney, R. L. 1988. Structuring objectives for problems of public interest. Operations Research, 36 (3), pp. 396–405.

Keeney, R. L., Winterfeldt, D. V., & Eppel, T. 1990. Eliciting Public Values for Complex Policy Decisions. *Management Science, 36* (9), pp. 1011-1030.

Keeney, R. L. 1992. Value-Focused Thinking: A Path to Creative Decision making. Harvard University Press.

Keeney, R.L. 1994a. Creativity in decision making with value-focused thinking. Sloan Management Review, 35, pp. 33–41.

Keeney, R. L. 1994b. Using Values in Operations Research. *Operations Research,42*(5), pp. 793-813.

Keeney, R. L. 1996. Value-focused thinking: Identifying decision opportunities and creating alternatives. European Journal of Operational Research, 92 (3), pp. 537–549.

Keeney, R.L. 1999. The value of Internet commerce to the customer. Management Science, 45, pp. 533–542.

Keeney, R. L. & Gregory R. S. 2005. Selecting attributes to measure the achievement of objectives. Operations Research, 53 (1), pp. 1–11.

Keeney, R. L. 2006. Eliciting Knowledge About Values For Public Policy Decisions. *International Journal of Information Technology & Decision Making, 05* (04), pp. 739-749.

Keeney, R. L. 2013. Foundations for Group Decision Analysis. *Decision Analysis, 10* (2), pp. 103-120.

Keeney, R. L., & Palley, A. B. 2013. Decision Strategies to Reduce Teenage and Young Adult Deaths in the United States. *Risk Analysis, 33* (9), pp. 1661-1676.

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. 2013. Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International journal of human-computer studies, 71* (12), pp. 1163-1173.

King, J., Patel, V., Jamoom, E. W., & Furukawa, M. F. 2014. Clinical benefits of electronic health record use: national findings. *Health services research*, *49* (1 pt2), pp. 392-404.

Kim, C., Tao, W., Shin, N., & Kim, K. S. 2010. An empirical study of customers' perceptions of security and trust in e-payment systems. *Electronic commerce research and applications*, *9* (1), pp. 84-95.

Kirkwood, C. W. 1997. Strategic Decision Making, Multi-objective Decision Analysis with Spreadsheets. Belmont: Wadsworth Publishing Company.

Klein, H.K. & Myers, M.D. 1999. A set of principles for conducting and evaluating interpretive field studies in information systems. MIS Quarterly, 23, pp. 67–94.

Kokolakis, S. 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, pp. 122-134.

Kordzadeh, N. 2014. *Communicating personal health information in virtual health communities: An integration of privacy calculus model and affective commitment*. The University of Texas at San Antonio.

Kwon, J., & Johnson, M. E. 2014. PROACTIVE VS. REACTIVE SECURITY INVESTMENTS IN THE HEALTHCARE SECTOR. M*ISQ*, *38*(2), pp. 451-471.

Lee, K. (2016, June 21). HIPAA violation examples: The five most common mistakes. Retrieved January 12, 2018, from http://searchhealthit.techtarget.com/photostory/450298831/HIPAA-violation-examples-The-five-most-common-mistakes/4/Healthcare-data-security-Lack-of-transmission-security-encryption

Lee, C. H., Geng, X., & Raghunathan, S. 2016. Mandatory standards and organizational information security. *Information Systems Research, 27*(1), pp. 70-86.

Li, X. B., & Qin, J. 2017. Anonymizing and sharing medical text records. *Information Systems Research, 28*(2), pp. 332-352.

Linden, H. V., Kalra, D., Hasman, A., & Talmon, J. 2009. Inter-organizational future proof EHR systems. *International Journal of Medical Informatics, 78* (3), pp. 141-160.

Lienert, J., Duygan, M., & Zheng, J. 2016. Preference stability over time with multiple elicitation methods to support wastewater infrastructure decision-making. European Journal of Operational Research, 253(3), pp. 746-760.

Lowry, P. B., Dinev, T., & Willison, R. 2017. Why security and privacy research lies at the centre of the information systems (IS) artefact: proposing a bold research agenda. *European Journal of Information Systems, 26* (6), pp. 546-563.

Lowry, P. B., & Moody, G. D. 2015. Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. *Information Systems Journal, 25*(5), pp. 433-463.

Lowry, P. B., Posey, C., Bennett, R. B. J., & Roberts, T. L. 2015. Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust. Information Systems Journal, 25(3), pp. 193-273.

Martínez-Pérez, B., De La Torre-Díez, I., & López-Coronado, M. 2015. Privacy and security in mobile health apps: a review and recommendations. *Journal of medical systems*, *39* (1), pp. 181.

May, J., Dhillon G., & Caldeira M. 2013. Defining value-based objectives for ERP systems planning. Decision Support Systems, 55 (1), pp. 98–109.

Meingast, M., Roosta, T., & Sastry, S. 2006. Security and privacy issues with health care information technology. In *Engineering in Medicine and Biology Society, 2006. EMBS'06. 28th Annual International Conference of the IEEE* (pp. 5453-5458). IEEE.

Merrick, J. R., & Garcia, M. W. 2004. Using Value-Focused Thinking to Improve Watersheds. *Journal of the American Planning Association, 70* (3), pp. 313-327.

Merrick, J. R., Parnell, G. S., Barnett, J., & Garcia, M. 2005a. A Multiple-Objective Decision Analysis of Stakeholder Values to Identify Watershed Improvement Needs. *Decision Analysis, 2* (1), pp 44-57.

Merrick, J. R., Grabowski, M., Ayyalasomayajula, P., & Harrald, J. R. 2005b. Understanding Organizational Safety Using Value-Focused Thinking. *Risk Analysis, 25* (4), pp. 1029-1041.

Miltgen, C. L., & Smith, H. J. 2015. Exploring information privacy regulation, risks, trust, and behavior. Information & Management, 52 (6), pp. 741-759.

Moulton, B., & King, J. S. 2010. Aligning ethics with medical decision-making: the quest for informed patient choice. The Journal of Law, Medicine & Ethics, 38(1), pp. 85-97.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. 2009. What levels of moral reasoning and values explain adherence to information security rules? An empirical study. European Journal of Information Systems, 18(2), pp. 126-139.

Nissenbaum, H. 2004. Privacy as Contextual Integrity. *Washington Law Review*, 79 (1), pp. 119-158.

Patel, V., Beckjord, E., Moser, R. P., Hughes, P., & Hesse, B. W. 2015. The Role of HealthCare Experience and Consumer Information Efficacy in Shaping Privacy and

Security Perceptions of Medical Records: National Consumer Survey Results. *JMIR Medical Informatics, 3* (2).

Patil, H. K., & Seshadri, R. 2014. Big data security and privacy issues in healthcare. In *Big Data (BigData Congress), 2014 IEEE International Congress on* (pp. 762-765). IEEE.

Phythian, G.J. & King, M. 1992. Developing an Expert System for tender enquiry evaluation: a case study. European Journal of Operational Research, 56, pp. 15–29.

Pielke Jr., R.A., Sarewitz, D. & Byerly Jr., R. 2000. Decision making and the future of nature: understanding and using predictions. In: Sarewitz, D., Pielke, Jr., R.A., Byerly, Jr., R. (Eds.), Prediction: Science, Decision Making, and the Future of Nature. Island Press, Washington, DC, pp. 361–387.

Pinsonneault, A., & Kraemer, K. 1993. Survey Research Methodology in Management Information Systems: An Assessment. *Journal of Management Information Systems*, *10* (2), pp. 75-105.

Paquette, S., Jaeger, P. T., & Wilson, S. C. 2010. Identifying the security risks associated with governmental use of cloud computing. Government information quarterly, 27(3), pp. 245-253.

Pavlou, P. A. 2011. State of the information privacy literature: Where are we now and where should we go? *MIS quarterly*, pp. 977-988.

Ross, S. E., & Lin, C. T. 2003. The effects of promoting patient access to medical records: a review. *Journal of the American Medical Informatics Association*, *10*(2), pp. 129-138.

Saaty, T. L. 1980. The Analytic Hierarchy Process, NY. McGraw-Hill, USA. Cook WD and Seiford LM.(1978). Priority ranking and consensus formation, Management Science, 24, pp. 1721-1732.

Sankar, P., Moran, S., Merz, J.F. & Jones, N.L. 2003. 'Patient perspectives on medical confidentiality: a review of the literature', Journal of General Internal Medicine, Vol. 18, pp. 659–669.

Sarewitz, D., & Pielke, R. A. 2007. The neglected heart of science policy: reconciling supply of and demand for science. *environmental science & policy*, *10*(1), 5-16.

Sarewitz, D., Pielke, Jr., R.A., Byerly, Jr., R. (Eds.). 2000. Prediction: Science, Decision Making, and the Future of Nature. Island Press, Washington, DC.

Secretary, HHS. O., & OCR, O. F. 2013. Summary of the HIPAA Security Rule. Retrieved July 16, 2017, from https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

Secretary, HHS. O., & OCR, O. F. 2017. HITECH Act Enforcement Interim Final Rule. Retrieved July 16, 2017, from https://www.hhs.gov/hipaa/for-professionals/special-topics/HITECH-act-enforcement-interim-final-rule/index.html

Siponen, M., Pahnila, S., & Mahmood, A. 2007, May. Employees' adherence to information security policies: an empirical study. In IFIP International Information Security Conference (pp. 133-144). Springer, Boston, MA.

Siponen, M., & Willison, R. 2009. Information security management standards: Problems and solutions. Information & Management, 46 (5), pp. 267-270.

Smith, H.J. (1993). "Privacy policies and practices: inside the organizational maze," Communications of the ACM (36:12), pp. 104-122.

Smith, H. J., Dinev, T., & Xu, H. 2011. Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*,*35*(4), pp. 989-1015.

Son, J. Y. 2011. Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management, 48* (7), pp. 296-302.

Spears, J. L., & Barki, H. 2010. User participation in information systems security risk management. *MIS quarterly*, pp. 503-522.

Straub Jr, D. W. 1990. Effective IS security: An empirical study. *Information Systems Research, 1* (3), pp. 255-276.

Sumner, M. 2009. Information security threats: a comparative analysis of impact, probability, and preparedness. Information Systems Management, 26 (1), pp. 2-12.

Topol, E. J. 2015. *The patient will see you now: the future of medicine is in your hands*. Tantor Media.

Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. 2011. The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research, 22* (2), pp. 254-268.

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. 2015. Managing the introduction of information security awareness programmes in organisations. European Journal of Information Systems, 24 (1), pp. 38-58.

van der Vaart, R., Drossaert, C. H., Taal, E., Drossaers-Bakker, K. W., Vonkeman, H. E., & van de Laar, M. A. 2014. Impact of patient-accessible electronic medical records in rheumatology: use, satisfaction and effects on empowerment among patients. *BMC musculoskeletal disorders*, *15*(1), pp. 102.

Wall, J.D., Lowry, P.B., & Barlow, J. 2016. Organizational violations of externally governed privacy and security rules: Explaining and predicting selective violations under conditions of strain and excess. *Journal of the Association for Information Systems*, 17 (1), pp. 39-76.

Wang, J., Xiao, N., & Rao, H. R. 2015. Research Note—An Exploration of Risk Characteristics of Information Security Threats and Related Public Information Search Behavior. Information Systems Research, 26 (3), pp. 619-633.

Warkentin, M., & Willison, R. 2009. Behavioral and policy issues in information systems security: the insider threat. European Journal of Information Systems, 18 (2), pp. 101-105.

Walsham, G. 1995. Interpretive case studies in IS research: nature and method. European Journal of Information Systems, 4, pp. 74–81.

Westin, A. F., & Ruebhausen, O. M. (2015). *Privacy and freedom*. Ig Publishing.

Williams, H., Spencer, K., Sanders, C., Lund, D., Whitley, E. A., Kaye, J., & Dixon, W. G. 2015. Dynamic consent: a possible solution to improve patient confidence and trust in how electronic patient records are used in medical research. *JMIR medical informatics*, *3*(1).

Witesman, E. M., & Walters, L. C. 2014. Modeling Public Decision Preferences Using Context-Specific Value Hierarchies. *The American Review of Public Administration*, *45* (1), pp. 86-105.