Journal of the Association for Information Systems

Volume 22 | Issue 4 Article 6

2021

An Activity Theory Approach to Leak Detection and Mitigation in Patient Health Information (PHI)

Rohit Valecha
University of Texas at San Antonio, rvalecha6446@gmail.com

Shambhu Upadhyaya
State University of New York at Buffalo, shambhu@cse.Buffalo.EDU

H. Raghav Rao
University of Texas at San Antonio, hr.rao@utsa.edu

Recommended Citation
Valecha, Rohit; Upadhyaya, Shambhu; and Rao, H. Raghav (2021) "An Activity Theory Approach to Leak Detection and Mitigation in Patient Health Information (PHI)," *Journal of the Association for Information Systems*, 22(4), .
DOI: 10.17705/1jais.00687
Available at: https://aisel.aisnet.org/jais/vol22/iss4/6

Journal of the Association for Information Systems (2021) **22**(4), 1007-1036
doi: 10.17705/1jais.00687

RESEARCH ARTICLE

ISSN 1536-9323

An Activity Theory Approach to Leak Detection and Mitigation in Patient Health Information (PHI)

Rohit Valecha[1], Shambhu Upadhyaya[2], H. Raghav Rao[3]

[1]University of Texas at San Antonio, USA, rvalecha6446@gmail.com
[2]State University of New York at Buffalo, USA, shambhu@cse.buffalo.edu
[3]University of Texas at San Antonio, USA, hr.rao@utsa.edu

Abstract

The migration to electronic health records (EHR) in the healthcare industry has raised issues with respect to security and privacy. One issue that has become a concern for healthcare providers, insurance companies, and pharmacies is patient health information (PHI) leaks because PHI leaks can lead to violation of privacy laws, which protect the privacy of individuals' identifiable health information, potentially resulting in a healthcare crisis. This study explores the issue of PHI leaks from an access control viewpoint. We utilize access control policies and PHI leak scenarios derived from semi structured interviews with four healthcare practitioners and use the lens of activity theory to articulate the design of an access control model for detecting and mitigating PHI leaks. Subsequently, we follow up with a prototype as a proof of concept.

Keywords: Patient Health Information (PHI), PHI Leak Detection and Mitigation, Activity Theory, Access Control Model, Design Science, Crisis Management

Tom Stafford was the accepting senior editor. This research article was submitted on May 7, 2019 and underwent two revisions.

1 Introduction

The adoption of digital patient records, government initiatives to move such records online, and the need for information exchange between patients, providers, and payers has increased the risk of patient health information (PHI[1]) leaks (Sokolova et al., 2009). A 2015 report by Verizon, drawing from 392 million security incidents and 1,931 data breaches across 25 nations, notes that 90% of industries have leaked PHI.[2] Given the integration of data across sources in healthcare networks, PHI leaks are becoming a major security issue (Hu et al., 2010). In some cases, PHI leaks result in privacy violations and social stigmatization (Wimmer et al., 2016); in other cases they may lead to medication errors and insurance fraud (Johnson & Wiley, 2011), potentially resulting in a healthcare crisis. Given these issues, the academic literature on PHI leaks is growing.

In this paper, we follow prior literature and define PHI leak as the inappropriate (inadvertent/unintentional or intentional) or unauthorized disclosure of patient information to an untrusted user (Johnson & Wiley, 2011; Shabtai et al., 2012). PHI leaks and unauthorized disclosures have been attributed to access violations (Broghammer, 2017), and Johnson (2009) states that

[1] In the literature, PHI is used to refer to patient health information, personal health information, and protected health information. In this paper, we use these terms interchangeably to avoid monotony.

[2] http://www.verizonenterprise.com/resources/reports/rp_2015-protected-health-information-data-breach-report_en_xg.pdf

controlling access to PHI is a necessary first step in the protection of PHI. Appari and Johnson (2010) urge organizations to enact better information control since expanded access increases information security risks (Ho and Warkentin, 2017). Access violations relating to PHI are serious problems in and of themselves that expose organizations to civil lawsuits and regulatory sanctions and can damage public relations.

The healthcare literature details access control issues related to the PHI leak problem, including controlling access to file-sharing applications (Emam et al., 2010), controlling access in risky workaround situations (Johnson & Wiley, 2010), and controlling the access of users (Smari et al., 2014). Missing from this literature are models to support the design of access control models for PHI leak detection and mitigation. Based on these observations, we offer the following research question:

RQ: How can access control models be designed for PHI leak detection and mitigation?

In this paper, we adopt the design science research method (Hevner et al., 2004) to articulate the design of an access control model (ACM) to aid in the detection and mitigation of PHI leaks and manage potential healthcare crises.

We suggest that one potential solution is that the design of access control models (ACM) should incorporate a perspective that includes technical safeguards and policies (Johnson, 2009). We use the lens of activity theory to build the framework that drives this paper. The value of a model based on activity theory is that it can be used to model real-world complex domains (Chaudhary et al., 2001; Wand and Weber, 2002). It provides the foundations needed to define a modeling language with symbols and vocabulary that can serve as the building blocks from which more complex expressions can be articulated (Rees & Barkhi, 2001; Tremblay et al., 2014).

This paper makes a twofold contribution: First, we adapt activity theory and utilize access control policies from real-world data to propose the design and specification of access control models for use in modeling PHI leaks. Second, we gather PHI leak scenarios from healthcare practitioners and adapt activity theory, restructuring the constituents of an activity system to incorporate "request" and "response" interactions. This restructuring allows us to capture a view of access control systems required for PHI leak detection and mitigation. We follow this with a prototype as a proof of concept (Peffers et al., 2007). This paper fits the representation genre (Parsons & Wand, 1997) of design science (Rai, 2017).

In the next section, we discuss the background of PHI leaks and access control. Then, we focus on the theoretical underpinnings of activity theory. Subsequently, we elaborate the design of our activity theory-based access control model for detecting and mitigating PHI leaks. We validate the model in the evaluation section, and then provide a brief overview of the prototype developed for PHI leak detection and mitigation. In the conclusion, we state the limitations of this work and suggest future directions.

2 Background

Electronic health records (EHRs) facilitate the collection and reporting of various metrics and behaviors on multiple individuals at different time points at a fraction of the cost of traditional paper-based approaches. EHRs provide accurate, up-to-date, and complete information about patients at the point of care, which can be used to predict a wide range of clinical outcomes (Cebul et al., 2011; Goldstein et al., 2017). However, some of the opportunities afforded by EHRs are overshadowed by severe problems related to PHI leaks. In this section, we discuss the background of PHI leak detection and mitigation in the context of access control.

2.1 PHI Leak Detection and Mitigation

PHI leaks come from many different sources. Johnson and Wiley (2010) identify ambulatory healthcare providers, acute-care hospitals, physician groups, medical laboratories, insurance carriers, back offices, and outsourced service providers, such as billing, collection, and transcription firms as sources. PHI leaks can be found throughout the healthcare chain, and involve care providers, laboratories, and financial partners, among other actors (Johnson & Wiley, 2011). Leaks are primarily caused by out-of-date systems or by inappropriate use due to improper employee training, negligence, or human error[3] (for example, lost or stolen laptops and flash drives have constituted sources of leaked sensitive patient information—Johnson & Wiley, 2011).

Numerous tools and systems have been developed in order to detect and mitigate information leaks (Alneyadi et al., 2016; Shibtai et al., 2012). Previous studies recommend technologies for data tracking and network monitoring to trace the flow of sensitive data, as well as technologies for data sanitizing, including disk-level encryption, tokenization, and data truncation (Johnson, 2009; Johnson & Wiley, 2011). Other studies have proposed a broad arsenal of enabling technologies, such as firewalls, identity management, etc. (Kale & Kulkarni, 2012; Papadimitriou & Garcia-Molina, 2011). Table 1 provides example cases of PHI leaks, along with information detailing how these leaks were detected and mitigated.

[3] We would like to thank an anonymous reviewer for pointing this out.

Table 1. Examples of PHI Leak Detection and Mitigation

#	Scenario	How the leak happened	How the leak was detected	How the leak was mitigated
1	Leaked health information of a celebrity[a]	Employee borrowed the credentials of three doctors	The leak was detected from the alerts raised by inappropriate access	Institution of a policy, i.e., those with high profile access should not share their passwords with other employees
2	Leaked names, date of births, and social security numbers from patients at a hospital[b]	Employee stole personal information from the billing application	Patient information was used to open credit card accounts and cellphone accounts	Patients were notified patients, offered free credit monitoring for one year, and a call center was set up

[a] http://healthitsecurity.com/news/kim-kardashians-patient-data-breached-at-cedars-sinai
[b] http://www.observeit.com/blog/umass-memorial-insider-breach-went-12-years

Table 2. PHI Leak

		Does the subject have access?	
		No	**Yes**
Is the subject authorized?	**No**	No leak	PHI leak—focus of this study
	Yes	Admin error (No leak)	No leak (legitimate access)

The predominant approaches for detecting and mitigating information leaks are content-based or behavior-based approaches (Katz et al., 2014; Soumya and Smitha, 2014). The content-based approach uses various rules that are defined for certain keywords, phrases, or terms (entities such as users, places, data, etc.) that may appear in a scanned text (Gafny et al., 2011). The rules determine a confidence score based on the number of times these keywords appear in the scanned text. Using confidence scores, the content-based approach seeks to identify sensitive content and then determine the level of threat its leakage may present to the organization (Harel et al., 2010). The behavior-based approach focuses on identifying anomalies in user behavior, which can be used to track illegitimate access to personal data (Lien et al., 2011) or access to other files (Mathew et al., 2010). The behavior-based method defines normal user behavior and issues an alert whenever a user's behavior deviates from the normal profile (Gafny et al., 2011).

Protecting against PHI leakage not only seeks to protect critical files and data, but also aims to ensure proper access control by determining who has access to what information and constantly reviewing access control settings (Table 2 shows how access control is related to PHI leaks). In summary, proper access control is essential for mitigating the risk of PHI information leaks (Broghammer, 2017). In line with this discussion, this paper suggests an access control solution for the PHI leak problem (i.e., for detecting and mitigating information leaks in the healthcare context).

Access control is the "process of mediating request to data and determining if the request should be granted or denied" (Valecha et al., 2014, p. 3). Milutinovic (2008) defines access control in the healthcare setting as the process of authorization in which the access to medical records can be limited to users with an appropriate role and allowed only during an episode of care. Access control involves three main entities: subject, resource, and action.

2.2 The Access Control Model (ACM)

The subject requests an action regarding a resource (Park & Ho, 2004). The ACM is generally expressed in terms of the subject, along with permissions in terms of various objects. The task of a subject is to access (read, write, etc.) objects, for which access is allowed or denied based on the permissions issued between subjects and objects listed in the relevant policy (Smari et al., 2014).

Table 3 lists some of the popular healthcare access control models. A majority of the access control models in the healthcare setting focus on the requestor in the context of patient data access requests. Fernández-Alemán et al. (2013) identify role-based access control (Sandhu et al., 1996) as "the access control model par excellence" (p. 549). Over the years, various other components such as affiliation, location, time, etc. have been incorporated into access control models in the healthcare setting (Beznosov, 1998). This evolution of access control models is in line with the work of other researchers who argue in favor of considering contextual factors that are a part of various business processes (Rosemann et al., 2008) by using access control models that utilize fine-grained access policies.

Table 3. Access Control Models in Healthcare Setting

Citation	Theory base	Access control elements
Beznosov (1998)	Role-based access control	Role, affiliation, location, time
Motta & Furuie (2003)	Role-based access control	Role, info, access, environment
Blobel (2004)	Policy-based access control	Role, info, access
American National Standard (2005)[a]	Role-based access control	Role, info, access
Rostad & Edsberg (2006)	Role-based access control	Role, info, reason, membership
Lovis et al. (2007)	-	Role, profile, access, department, time
Rostad (2008)	Role-based access control	Role, profile, access
Peleg et al. (2008)	Role-based access control	Roles and their relations, Info, Situation
Falcao-Reis et al. (2008)	Policy-based access control with OASIS and XACML	Role, info, access, situation
Ardagna et al. (2010)	Policy-based access control	Subject, object, access, environment
This paper	Activity theory-based access control	Subject, resource, community, rules, tools, division of labor, and interactions

[a] Standard Guide for Information Access Privileges to Health Information, http://www.astm.org/Standards/E1986.htm.

2.3 Access Control Requirements for PHI Leak Detection and Mitigation

Access control models in healthcare need to be extended to support complex healthcare requirements (Peleg et al., 2008). First, ACMs should permit a collective understanding of the users, processes, and technology (Garg et al., 2005) that relate to the "who, what, why, where, when, and how" of the context and are needed to address the PHI leak problem (Raman et al., 2011). Second, ACMs need to be flexible enough to allow for the consideration of interaction aspects (emergence of interactive entities) in addition to structural aspects (van der Haak et al., 2003). Furthermore, ACMs should enable consideration of work processes, organizational structure, and organizational environment and culture (Appari & Johnson, 2010; Ferreira et al., 2006).

While some access control models in healthcare settings consider context elements based on contextual data or environmental attributes (Mohan & Blough, 2010), they often lack information about how access control models can be designed for leak detection and mitigation. In particular, there is a need to identify specific ways in which access control models can be redesigned (or transformed) with a specific focus on leak detection and mitigation. To this end, it will be useful to deconstruct an access control model in order to identify the constituents involved in the leak detection and leak mitigation process and then realign the constituents into a reimagined access control model (which is further elaborated in the following subsection).

2.4 Need for Activity Theory (AT)

Figure 1 depicts a typical healthcare situation. All authorized users are allowed to obtain, change or delete patient data. There may be many different parties who need access to information, including patients, patients' family members, and professionals such as primary care physicians, physician's assistants, hospital personnel, doctors, nurses, specialists, pharmacists, researchers, scientists, dieticians, public health officials, paramedics, insurance agents, etc. Further, multiple devices enable access to multiple users within the workflow. Healthcare devices collect, store and report information from sensors using apps that can be used for diagnosis and treatment and enable patients to monitor and manage their health conditions.

In the healthcare access control scenario, it is important to realize that access happens in the context of interactions. A natural starting point is the interaction between the patient and the physician (Engeström, 1987). In terms of patient data, the constellation becomes more complex when the physician interacts with support staff and other hospital personnel in the hospital. In this scenario, the access requester and access provider form two separate but interactive parties within the access control system. The objective of the access requester is to perform patient tasks involving patient data, while the objective of the access provider is to deliver relevant information. When the two systems interact, the result is a shared objective—namely, acquiring the access needed to achieve the outcome of healthcare services provided to the patient.

Each interacting user may have asymmetric and dynamically changing demands regarding diverse patient data accessed from multiple apps, services, and devices. Each user may have different perspectives on how to perform a number of interrelated and overlapping activities using shared patient data, demonstrating that access control is a process of dialogic interaction that includes user participation and feedback.

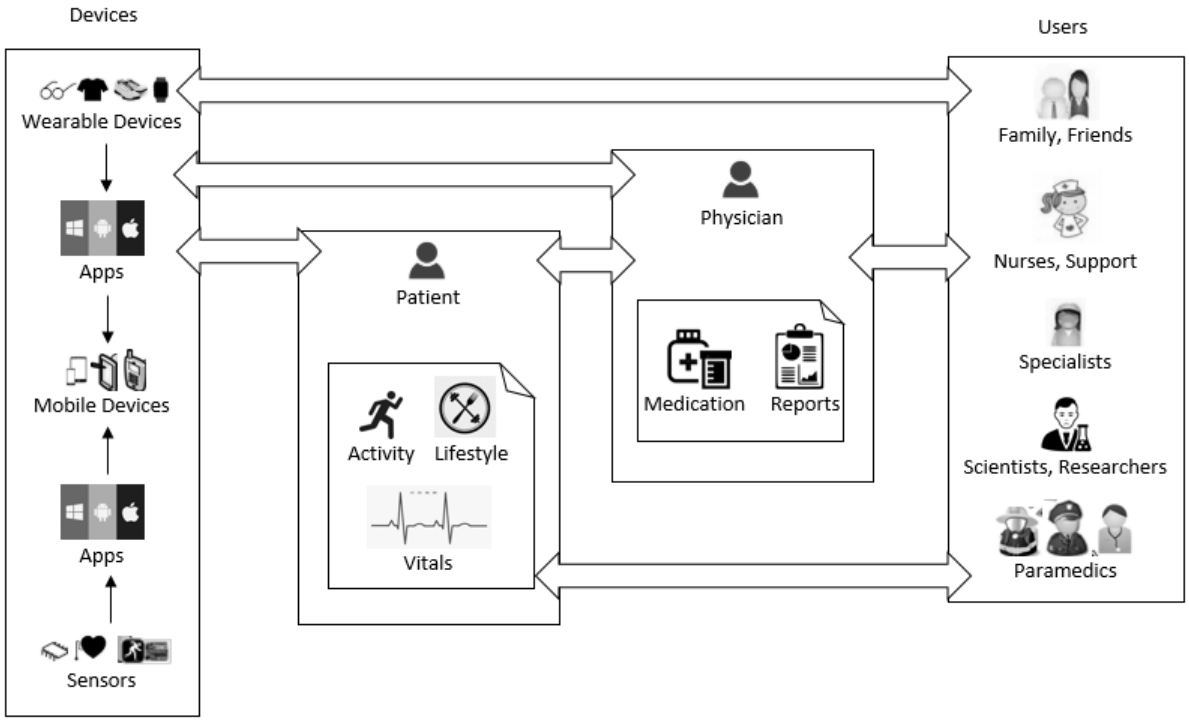


Figure 1. Health Access Components

Furthermore, access is not static but dynamic—i.e., it changes and develops in response to new access based on existing access. The problem of conflict arises when new access conflicts with existing access. As a result, private information becomes vulnerable to PHI leaks arising from conflicts caused by inadequate, inaccurate, or careless access control in data-intensive healthcare settings involving multiple users and devices.

In line with the need for "theories related to human knowledge" that can be used as "foundations for conceptual modelling in systems development" (Wand et al., 1995; p. 285), we propose activity theory (AT) as a framework to inform the design of access control models (Chen et al., 2008; Igira, 2008; Kaptelinin et al., 1995; Korpela et al. 2001; Valecha et al., 2014). We develop an AT-based access control model that incorporates contextual aspects of the healthcare situation and provides a sociotechnical perspective on PHI leak detection and mitigation (Allen et al., 2013; Ho et al., 2016; Karanasios et al., 2013; Volkoff et al., 2007).

By enabling analysis of complex situations, AT facilitates a unifying perspective that goes beyond traditional access control models. ACMs focus on the process of information exchange surrounding the information resource, while AT deals with the purpose of information exchange. ACMs use static structures to model access to the resource, and AT allows the modeling of dynamic interactions between agents. ACMs are resource centered whereas AT is "user-centered" in that it is generally oriented toward the subject and fosters mediated interaction within the flow of actions. The use of the AT approach allows us to focus on human-centered, positive design (Avital et al., 2006) and enables the analysis of the health information workflow as an activity-centric and agent-centric process (Raghu et al., 2004).

2.5 Activity Theory

Previous research has proposed that activity theory can be used as a theoretical framework to study context (Nardi, 1995) and provides a lens to deconstruct interactions within complex situations (Chen et al., 2008; Igira, 2008; Kaptelinin et al., 1999). AT enables the analysis of an organization's activity (Chen et al., 2013). In AT, the minimal unit of analysis is the activity system (Kuutti, 1996), involving an activity consisting of a subject directed toward an object.

AT has been extended through three generations of research (Tran et al., 2019). In the first generation of AT research, Vygotski and Leont'ev conceptualized the core of an activity as consisting of subjects, objects, and the mediating effect of tools that can be used by subjects to achieve the object in order to conduct the activity (Leont'ev, 1978; Vygotski, 1978). The subject is an individual or a group that performs the activity. The object can be either a material object or personal objectives (motives) (Fuentes et al., 2004; Nardi, 1995). The activity is supported by the means of physical or logical instruments.

In the second generation of AT research, Engeström focused on collective activities within a cultural and historic context by considering the mediating effect of rules, community, and the division of labor (Engeström, 1999, 2009; Kaptelinin et al., 1995). The community specifies the aspects of the external environment and includes multiple individuals who collaborate to act on the same general object (Jonassen, 2000). The key aspect of the community is that the community members have a common interest. The rules specify the logic or the boundaries for the activity, while the division of labor identifies the hierarchical responsibility (Valecha et al., 2014).

The third generation of AT focuses on interacting activity systems for investigating complex social activities to construct potential shared objects or objectives (Chen et al., 2013; Tran et al., 2020). In the third generation of AT research, multiple subjects are involved in various activities with separate but related objectives (Engeström, 1999, 2009). This activity is mediated by artifacts and is socially constituted within the surrounding environment (Bertelsen & Bødker, 2003; Vygotsky, 1978).

3 Access Control as an Activity System

In this section, we focus on the access control model and then adapt the access control model using activity theory based on the requirements of PHI leak detection and mitigation.

3.1 Basic Access Control Model

In an access control model, the basic element, the access control policy, comprises a target, obligation, and rules (see Figure 2). Together, this information is used to determine whether the policy is applicable to a given request. A matching function retrieves a value from the request, matching it with the values specified in the policy element according to the function's semantics. If the matching of an element succeeds for all categories, then the policy is applicable to the request (Margheri et al., 2013). The decision to permit or deny access is based on the matching function that determines whether the requested elements match the allowed elements (typically preset).

We utilize activity theory to deconstruct the access control activity, and investigate user access along the dimensions of the activity system: subject, activity, instrument, community, rule, and division of labor. We propose mapping the basic structure of an activity system onto a policy model of access control, which will facilitate an in-depth understanding of the access control policy and the associated business requirements and will allow us to recognize the key data elements in the access control context.

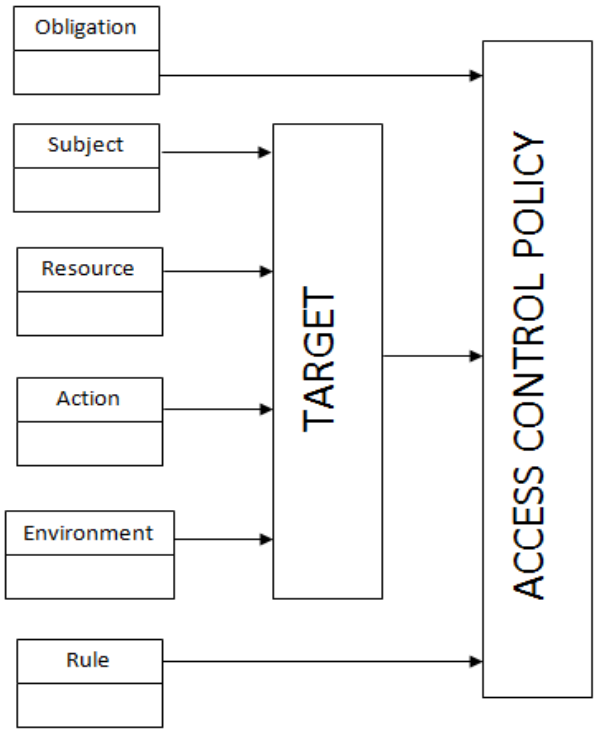


Figure 2. Access Control Policy Specification

Table 4. Access Control Policy Elements

Entity	Description
Access control policy	
Obligation	A set of parameters that the user is obligated to expose
Rule	A set of conditions that the request has to satisfy
Target	A set of attributes—subject, resource, action, environment—that the request has to consist of (see below)
Access control target	
Subject	The user requesting the access to the resource
Resource	The entity (i.e., patient data) being protected
Action	The operation to be performed on the resource
Environment	The setting in which the resource resides

3.2 Activity Theory-Based Access Control Model

To identify the aspects of AT-based analysis capable of enabling capture of a higher-level view of access control processes, we model access control in terms of activity components: i.e., subject, object, community, tools, rules, and division of labor. In an access control model, the subject performs the activity of requesting access to a resource that is typically some form of data or service. The obligation is the operation that is performed to enforce the authorization. The environment component specifies aspects of the external environment and provides other information. The rules identify a set of conditions that must be satisfied in order to obtain access. The action defines what type of access is requested for an object.

We argue that it is possible to map the basic structure of an activity onto an access control policy (see Figure 3). The subject and object factors contain information respectively associated with the subject and the access resource. The community factor includes details of the environment, such as the department (e.g., other personnel or support staff). The rules, division of labor (responsibility), and tools are related to sociotechnological factors associated with rules, social actions, and obligations (see Table 5). In an access control setup, the outcome can be accomplished through a decision mechanism for approving or denying access to PHI. This decision mechanism describes who can execute actions on patient resources and also explains how access can be constrained.

It is important to note that the conceptualization does not require a one-to-one mapping. Our view is that different interpretations exist depending on the context. For example, environmental information in one setting can be part of a rule in another setting. Likewise, the same piece of information can be part of different categories based on the activity. The same holds for the AT-based analysis itself: an object can function as a tool in different activity settings. We quote an anonymous reviewer in support of our argument that different components of the activity system can align with different factors of the access control model:

> *For example, [action] could equally be applied to rules, which also influence what actions are possible. The action itself, from an activity theory perspective, resides in the object because an activity theory object is not simply a thing, as in the data resource the subject is interested in accessing. Rather, it more broadly represents the goal of the subject, which in the access control model would include the action performed on the resource. In other words, the object for an activity theory subject in an access control scenario would be to gain access to data in order to do something with that data. Therefore, an accurate mapping would associate the object in activity theory with both the resource and action in the access control model.*[4]

This quote highlights that an object in the activity system can align with the resource and action factor in the access control model. In similar vein, the subject and division of labor components of the activity system can align with the subject factor in the access control model. Thus, the mapping from the activity system to the access control model suggests that activity theory can be used to specify access, allowing the designer to focus on task-related information (Valecha et al., 2014).

The basic principles of activity theory are important (Kaptelinin et al., 1999) for the design of the access control model for PHI leak detection and mitigation.

[4] We would like to thank an anonymous reviewer for pointing this out. We quote the reviewer's exact words in order to preserve its quintessential representation of the mapping of components of activity system with the different factors of the access control model.

Table 5. Sample Mapping of Activity System to Access Control System

Activity Theory aspects	Access control factors	Access governance and management
Subject, division of labor (responsibility)	Subject	Who has access?
Object	Resource, action	What data are sensitive?
Community	Environment	With whom is the data shared?
Rules	Rules	How are the data regulated?
Tools	Obligation	How are the data accessed?
Division of labor (responsibility)	Action	How do the data flow?

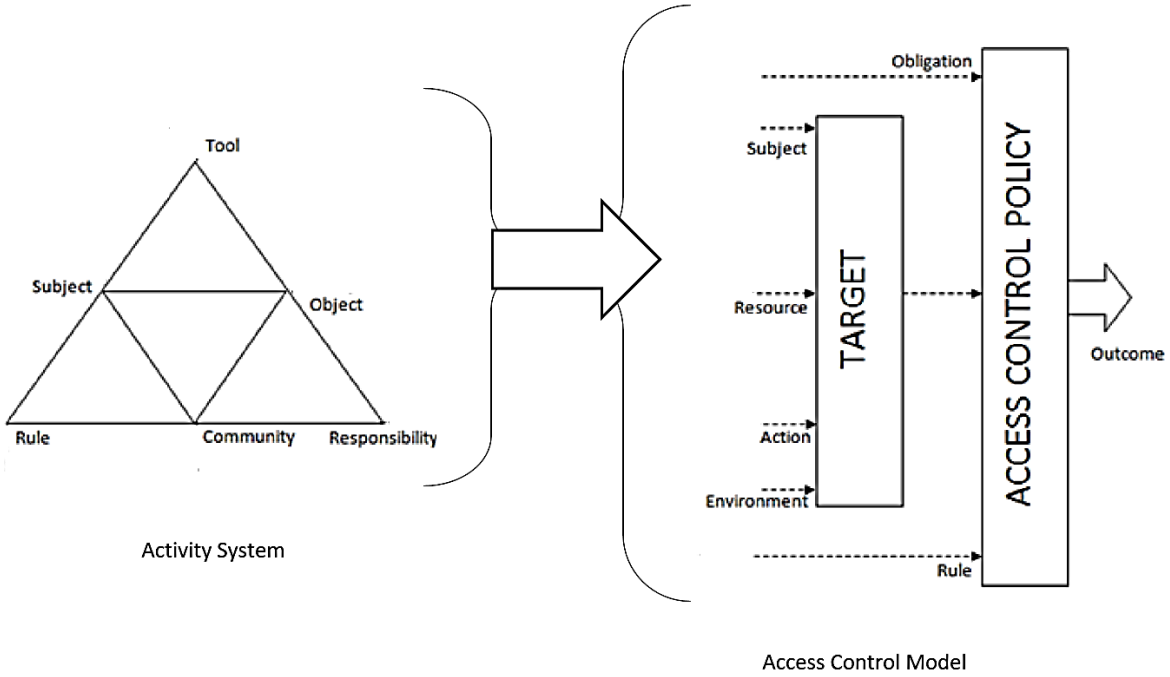


Figure 3. Activity Theory-Based Specification of Access Control Model

Thus, in order to explicate the elements within the access control model, we adapt the fundamental principles of AT as they relate to access control in the context of PHI leaks: namely, object-orientedness and mediation, multi-voicedness and context, historicity and emergence, and expansive transformation (Engeström, 2001; Kaptelinin et al., 1999).

Object-orientedness: The subject in the healthcare setting is the employee or the role that requires access to a patient's data. The employee's role determines the perspective from which the tasks are assumed by the access control model. The object in the access control model refers to a patient's data, and the objective is the employee's need to access this sensitive information from a hospital computer.

Tool-mediation: Access in the healthcare setting is facilitated through a work system within the hospital and the policies set up on that system for employee access. This system and its policies allow the employee to connect not only with the patient's data but also with other employees in the organization's community.

Multi-voicedness: As access is granted, various members of the health organization take the role of the subject. In this role, specialists and physicians or doctors may have different ideas and views about the access requested/provided to perform patient-related tasks. If access is insufficient, they may request/provide more access through a feedback mechanism. This feedback loop is particularly important to ensure that the goals of multi-voicedness, or multiple perspectives, are met. Multi-voicedness stems from the negotiation of access from different parties. This allows individual participants to bring their own unique experiences into the activity system.[5]

[5] We would like to thank an anonymous reviewer for pointing this out.

Historicity: Access control models maintain a selective history of the access requests made by individual hospital employees and utilize this history to improve the differentiation between safe and potentially dangerous requests (Edjlali et al., 1998). This history identifies access requests made in previous units of time and enables monitoring of the continuous spectrum of requests, from "declined" to "granted." Access can be granted or declined based on the evaluation of a history of activities of the requester, e.g., behavior, time between requests, content of requests, etc. (Schapranow, 2012).

Expansive transformation: Next-gen sensors and wearable devices that collect and store health information represent important transformations that require patients to learn new and previously unconsidered means of controlling access to their data. Also, healthcare workers must adjust to the practice of access control by designing and implementing workarounds, which requires an understanding of the structure of the access system and necessitates new interpretations of the purpose of access.

4 Designing Access Control Activity System for PHI Leak Detection and Mitigation

As mentioned earlier, Engeström (1987) describes an activity system as containing interacting components: subjects, object, tools, community, rules, and division of labor, which interact to attain the activity outcome. These components continually influence and transform one another through their interactions, which can happen within the activity system or between activity systems (Engeström, 1987). Prior research has investigated "between" activity system interactions, where multiple actors from different activity systems work together with other actors to effectively address a complex and rapidly evolving situation (e.g., Chen et al., 2013).

In an access control setting, multiple actors seek access in the context of working together with others—i.e., access is permitted or denied based on interactions of various individuals from different activity systems. Engeström has investigated between-activity system interactions in the healthcare domain (Engeström, 1987, 2019) but not in the context of access control. However, such interactions may also be applicable in the context of patient data access exchange.

Focusing on the key interactions between the activity system, we can reimagine the system by expanding the activity object (Kuutti, 1996). Interactions are key for activity restructuring and are important for incorporation into any access control model seeking to detect and mitigate PHI leaks. Below, we explicate the key interactions between user access control activities.

In a healthcare scenario, the starting point is the patient describing how access is to be granted in the community (by specifying how the access requester and the surrounding community should interact while accessing patient data). For example, a patient might give a specialist doctor (who works with a patient's primary care doctor) permission to access their diagnostic information (Peleg et al., 2008) in the context of an access request system involving interactions between access requesters and the community of doctors, nurses and hospital staff/personnel, all of whom are involved in the process of accessing patient data. This system generally identifies who has access to what resources (Fernández-Alemán et al., 2013).

However, the access requester might be involved in the interpretation/analysis of patient data or might need to share patient data. Thus, there needs to be rules that explicitly or implicitly guide the actions of access requesters (Brossard, 2011). Moreover, the requester may utilize any set of tools, sign systems, or procedures for acting on patient data; thus, there needs to an awareness of the resources and tools available for accessing patient data. Access requests can limit who can see what information, and can limit data to the information that the requester is entitled to see (Damiani et al., 2002). Prior studies have investigated various types of access requests, and Mohan and Blough (2010) argue that access requests should be specified through more detailed policies and rules.

In a security model, the system administrator defines the rules providing access to resource objects. These rules are often based on conditions such as time of day or location. In addition, access management systems can provide tools, such as access control software and user database tools to provide access. According to TechTarget, access is provided to the requester of the patient data using rules, tools/frameworks, and job responsibility workflows.[6] This represents the access response system, which sets control boundaries defining how tools are used to collect patient data, how community members divide work to achieve patient-related tasks, and the implicit and explicit norms that govern the relationships between the subject and those seeking access to patient data. Thus, in an access control setting, we consider "access request" and "access response" systems as interacting systems of the access control activity system (see Figure 4).

[6] https://searchsecurity.techtarget.com/definition/access-control

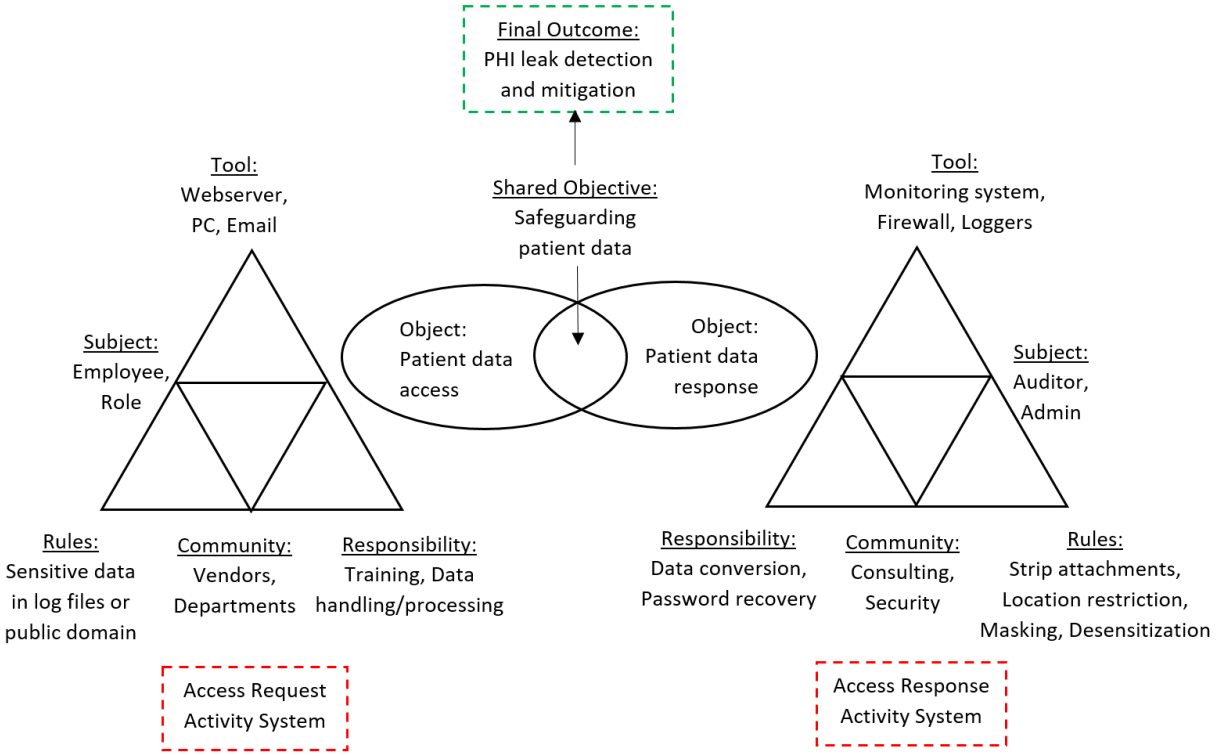


Figure 4. AT-Based Leak Detection and Mitigation Model

The access request system encapsulates employee behavior in various contexts, representing patient data according to a variety of personal factors and the department within the organization. Therefore, the access request system can facilitate the discovery of leak points across the network of the healthcare organization and can assist in the risk assessment function of the security system. Access request systems can also identify PHI leak patterns based on impacts on privacy and monetary losses.

The access response system can implement tactical controls for the leak points identified in the discovery process of PHI leak detection, allowing for the definition of different levels of security classification and the determination of appropriate levels of control (March and Scudder, 2017). The access response system can describe how controls and policies should be applied to medical instruments through rules and organizational hierarchies in a way that safeguards patient data.

The access request system can also track unauthorized access by comparing requests with permissions and can deny inappropriate requests. A key requirement for effective PHI leak detection and mitigation is ensuring that sensitive patient information is monitored within the healthcare organization. Therefore, access request and access response systems can identify PHI leak points and potential enforcement policies.

Table 6 presents the results of applying a third-generation AT-based leak detection and mitigation model to sample PHI leak scenarios of inappropriate or unauthorized disclosure (leaks) of patient information. For some scenarios, we used Google searches, using the keywords “PHI leaks,” “PHI leak case studies,” “Data breaches in healthcare,” and “PHI data breaches.” We also searched for PHI leak examples in the Identity Theft Resource Center (ITRC), an organization devoted to the mitigation of information theft. Finally, we searched for “access control” AND “scenarios” within all the studies cited in a literature review article written by Fernández-Alemán et al. (2013) that provides a systematic review of access control in healthcare settings. For other scenarios, we asked healthcare managers if they could provide examples of leaks. The objective of this process was to derive rich data about PHI leaks. During this process, more than 20 scenarios were collected (four of them are detailed in Table 6).

5 Evaluation

Models are tested through their usage and application (Chen et al., 2013). Connolly and Begg (2002) provide useful guidance on validating models (like the AT-based model discussed in this paper), and recommend validating models using two types of validation tasks: reviewing the model with users or testing transaction(s) against the model.

Table 6. PHI Leak Detection and Mitigation from Sample PHI Leak Scenarios

#	Scenario	PHI leak detection (access request)	PHI leak mitigation (access response)	Comments
1^	An employee copied the patient information files from the client server to a local machine in the vendor's office	*Subject:* Employee *Object:* Patient files *Comm:* Vendor *Rule:* Patient data moved *Tool:* Local machine *Div:* Data copy	*Subject:* Admin *Object:* De-sensitized files *Comm:* Vendor *Rule:* FTP access *Tool:* Local machine *Div:* Data transfer	• *Leak detected* based on data transfer to vendor • *Leak mitigated* through desensitization of patient data used in file transfer protocols
2	One of the vendors of a Medical center posted the patient data on their website[a]	*Subject:* Vendor *Object:* Patient data *Comm:* Internet *Rule:* Patient data online *Tool:* Webserver *Div:* Data posting	*Subject:* Medical center *Object:* Patient data *Comm:* Vendor *Rule:* Password protection *Tool:* Website *Div:* Data agreements	• *Leak detected* based on data transferred on to the internet • *Leak mitigated* through password protection of patient data stored on the websites
3	A clinician sends a newsletter to a group of 780 HIV patients' email addresses with names, email addresses[b]	*Subject:* Clinician *Object:* Names and emails *Comm:* Public *Rule:* Confidential data *Tool:* Option e-service *Div:* N/A	*Subject:* Admin *Object:* Personal data *Comm:* Patient *Rule:* Record masking *Tool:* Firewall *Div:* Training	• *Leak detected* based on data transferred to the public • *Leak mitigated* through record masking of data egressing out of the firewalls
4^	An employee uploaded log files with sensitive patient information to a vendor's website	*Subject:* Employee *Object:* Patient info *Comm:* Vendor *Rule:* Sensitive info in log *Tool:* Webserver *Div:* Log access	*Subject:* Auditor *Object:* Masked patient data *Comm:* Network *Rule:* Confidentiality *Tool:* FTP client Div: Data transfer	• *Leak detected* based on data transfer to vendors • *Leak mitigated* through confidentiality agreements on secure FTP

Note: ^ denotes PHI leak scenarios gathered from healthcare managers, "Comm" denotes community and "Div" denotes division of labor (responsibility).
[a] http://www.beckershospitalreview.com/healthcare-information-technology/boston-medical-center-vendor-posts-15-000-patients-information-online.html
[b] http://www.theguardian.com/technology/2015/sep/02/london-clinic-accidentally-reveals-hiv-status-of-780-patients

Participant review involves participants asked to review the model in whatever way they choose. Transaction testing includes events in the domain, referred to as transactions, which can be evaluated to determine whether they are represented in the model. Following Connolly and Begg's (2002) recommendations, we evaluated the model through both participant review and transaction testing using PHI leak scenarios to determine how well the model represents the domain.

5.1 Part 1: Evaluating the Activity Theory-Based Model for Specification of Access Control

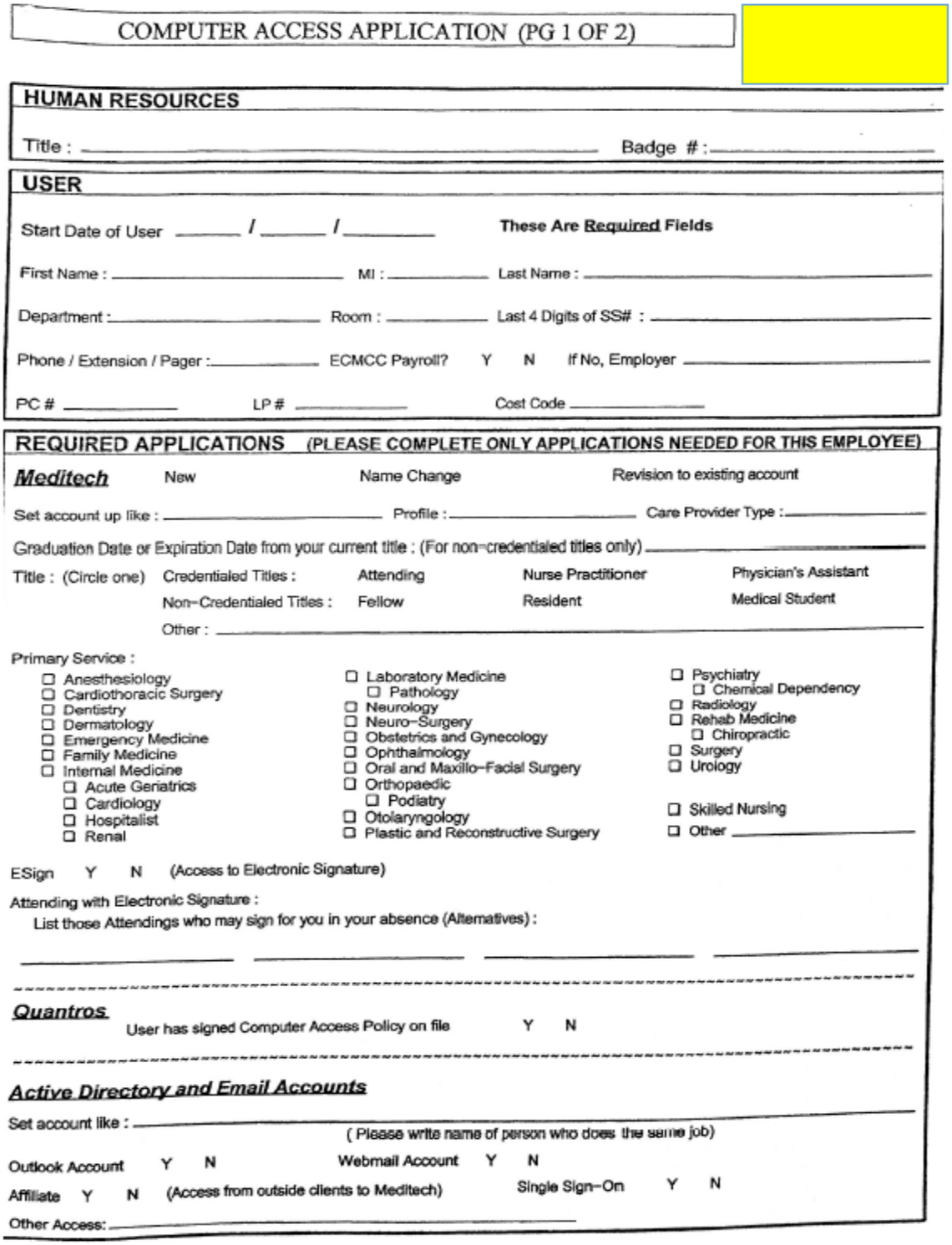
In this subsection, we discuss the methodology consisting of data collection and expert interviews to evaluate activity theory for the specification of access control policies.

5.1.1 Access Reports Data

We evaluated access control in the healthcare context using multiple sources of evidence. We collected access reports (see Figure 5) for users at different levels from healthcare organizations in central Tennessee (see Figure A1 in Appendix A) and western New York (see Figure A2 and A3 in Appendix A). These documents include fields for general information about the user, information about the applications utilized, and details about the service tasks. The data collection strategy allowed us to collect ample rich data related to access activities, resulting in the extraction of more than 100 access control policies from access reports for evaluation purposes.

5.1.2 Expert Interviews to Increase the Understanding of Access Reports

We interviewed healthcare professionals who had experience dealing with both PHI and access control. We contacted four healthcare managers from four different healthcare organizations with more than five years of experience dealing with access control. Two managers were from New York, one was from California, and one was from Tennessee. We conducted face-to-face interviews in New York and Tennessee and interviewed the manager from California by phone. We scheduled one or two interviews with each participant lasting 40-60 minutes over a period of a few weeks.



COMPUTER ACCESS APPLICATION (PG 1 OF 2)

HUMAN RESOURCES

Title : _____ Badge # : _____

USER

Start Date of User ____ / ____ / ____ **These Are Required Fields**

First Name : _____ MI : _____ Last Name : _____

Department : _____ Room : _____ Last 4 Digits of SS# : _____

Phone / Extension / Pager : _____ ECMCC Payroll? Y N If No, Employer _____

PC # _____ LP # _____ Cost Code _____

REQUIRED APPLICATIONS (PLEASE COMPLETE ONLY APPLICATIONS NEEDED FOR THIS EMPLOYEE)

Meditech New Name Change Revision to existing account

Set account up like : _____ Profile : _____ Care Provider Type : _____

Graduation Date or Expiration Date from your current title : (For non-credentialed titles only) _____

Title : (Circle one) Credentialed Titles : Attending Nurse Practitioner Physician's Assistant

Non-Credentialed Titles : Fellow Resident Medical Student

Other : _____

Primary Service :

- ☐ Anesthesiology
- ☐ Cardiothoracic Surgery
- ☐ Dentistry
- ☐ Dermatology
- ☐ Emergency Medicine
- ☐ Family Medicine
- ☐ Internal Medicine
  - ☐ Acute Geriatrics
  - ☐ Cardiology
  - ☐ Hospitalist
  - ☐ Renal
- ☐ Laboratory Medicine
  - ☐ Pathology
- ☐ Neurology
- ☐ Neuro-Surgery
- ☐ Obstetrics and Gynecology
- ☐ Ophthalmology
- ☐ Oral and Maxillo-Facial Surgery
- ☐ Orthopaedic
  - ☐ Podiatry
- ☐ Otolaryngology
- ☐ Plastic and Reconstructive Surgery
- ☐ Psychiatry
  - ☐ Chemical Dependency
- ☐ Radiology
- ☐ Rehab Medicine
  - ☐ Chiropractic
- ☐ Surgery
- ☐ Urology
- ☐ Skilled Nursing
- ☐ Other _____

ESign Y N (Access to Electronic Signature)

Attending with Electronic Signature :

List those Attendings who may sign for you in your absence (Alternatives) :

_____ _____ _____ _____

Quantros

User has signed Computer Access Policy on file Y N

Active Directory and Email Accounts

Set account like : _____

(Please write name of person who does the same job)

Outlook Account Y N Webmail Account Y N

Affiliate Y N (Access from outside clients to Meditech) Single Sign-On Y N

Other Access: _____

Figure 5. Access Request Reports from a New York Health Organization (Page 1 of 2)[7]

[7] For other access request reports, see Appendix A

Model validation involves the examination of its representativeness—i.e., how closely the model represents the domain. The model can be considered representative if it represents the domain accurately and completely. Therefore, during participant review, we asked the healthcare managers the following questions to determine how well AT allows for the formulation of access control policies: Does the AT model capture the following details about the access control policies: (1) who tried to access? (2) what data? (3) in what way? (4) other details of the setting? (5) Does the AT model allow for a complete representation of access control policies? (6) Does the model allow for an accurate representation of access control policies? These questions provided a means to confirm whether the model captures the various data access encounters that take place within the healthcare workflow (as evidenced by the access reports) involving medical staff providing healthcare services to patients.

5.1.3 Data Analysis of Access Reports

The data collection strategy allowed us to collect several access control policies from the access reports. For a partial list of activity elements from access reports, refer to Table 7. The process of evaluating activity theory for access control specification consisted of two steps: confirming pieces of information and the formation of categories. For example, let us consider the following description of access control provided by the healthcare manager from California: "an *employee* from *eligibility division* had emailed a *file* to the *corporate distribution list*."

An examination of the policy showed that it could be structured into patterns of activity. An AT-guided coding exercise helped reveal the structure of the activity consisting of the six components: subject, resource, community, tools, rules, and division of labor (Engeström, 1987). The AT-based model enabled us to highlight the informative pieces by focusing on the activity components, which allowed us to produce a rich descriptive account of how the PHI was organized within the PHI exchange.

Formation of the categories based on the identified information pieces comprised the second step. The AT-based model allowed us to group information pieces into categories based on the AT components. In the above example, the eligibility division is a department. AT provides the component of *community,* which allows different departments to be grouped together. Moreover, the patient's file was categorized as health data. AT provides the component of *object,* which allows different healthcare data items to be grouped together. This process revealed the emerging categories within the scenarios.

A key aspect of the data analysis process was identifying whether the AT-based model captured the information components and their interactions within the PHI sources. In this part of the evaluation, the authors provided the access control policies as well as the access control elements derived by using the AT-based model to the interviewed healthcare managers. The managers reviewed these elements by comparing the raw information with the structured information derived by applying the model. They confirmed that the information derived from the model accurately depicts health information workflows.

Prior literature has identified a number of approaches for access control. We performed a comparison with some of the popular approaches: role-based (Sandhu et al., 1996; Motta and Furuie, 2003), policy-based (Blobel, 2004), and situation-based (Peleg et al., 2008). Table 8 offers a comparative summary. The comparison suggests that the AT-based approach provides a more comprehensive framework for the specification of access control models. For example, a situation-based access control model includes abstractions for modeling the entities involved in a situation (patient, requestor, task, health records) (Peleg et al., 2008). However, the situation-based ACMs do not take abstractions related to processes (such as hierarchies) or interactions (such as contradictions) into account.

Table 7. Activity Elements from Access Reports

Activity Theory aspects	Sample elements from access request reports
Subject	User roles, user profiles, user properties, user membership
Object	Information metadata, patient data
Community	User department, user affiliation
Rules	Access mode, access obligations, situational elements
Tools	Medical devices, system modules
Division of labor (responsibility)	Hierarchical structure, organizational obligation

Table 8. Comparison of Approaches of Access Control

Dimension	Focus	Role-based	Policy-based	Situation-based	AT-based
People	Individual	X	X	X	X
	Community			X	X
Process	Task structure		X	X	X
	Division of labor				X
	Temporal sequence				X
	Object hierarchy				X
Technology	Instrument	X	X	X	X
	Information	X	X	X	X
	Social issues				X
	Environment issues		X	X	X
Interaction	Contradictions				X
	History			X	X

5.2 Part 2: Evaluating Activity Theory-Based Access Control Model for PHI Leak Detection and Mitigation

In this subsection, we discuss the methodology consisting of data collection and expert interviews for evaluating whether the activity theory-based access control model allows for the detection and mitigation of PHI leaks.

5.2.1 PHI Leak Scenarios Data

Following Peleg et al. (2008), who use scenarios of access requests to acquire a deeper understanding of PHI leaks, we sought to collect scenarios involving the inadvertent disclosure of patient information from the healthcare managers we contacted. Accordingly, we evaluated the PHI leak detection and mitigation model using the PHI leak scenarios that they provided. In this process, the managers clarified the details of the health information workflow in which the leak took place and evaluated healthcare activities, elements, and interactions.

The PHI leak scenario reports describe the details of the patient information flow process, and include information about the leak incident, information on the employee that resulted in the PHI loss, and information about the patient data compromised. These reports also documented disciplinary action against responsible employees and steps taken to prevent such incidents in the future. Because the reports include sensitive patient information, the healthcare managers we interviewed were unwilling to share the actual reports. However, they did share anonymized anecdotes about scenarios of the PHI leak incidents, as well as leak-related information regarding occurrence, detection, prevention, etc.

5.2.2 Expert Interviews for Understanding PHI Leak Scenarios

Interview questions primarily sought to gain a deeper understanding of the nature of PHI leaks and the processes and tools that healthcare managers use to detect and mitigate PHI leaks. We designed semistructured questions for the interviews, and organized the interviews by grouping questions into three themes: PHI leak, PHI leak detection, and PHI leak mitigation. The first author took notes while the managers responded to the questions. The notes were discussed with the other authors to check for clarity and any missing information. In cases where the notes lacked clarity, the authors reached out to the managers to request a subsequent interview for clarification purposes.

In the first round of interviews, we described the PHI leak based on a summary of prior cases in the literature—as an inadvertent disclosure of patient information—to the managers. Then, we gave them time to recollect a few incidents[8] they had experienced that fit the definition. Subsequently, we collected managers' descriptions of [PHI leak] incidents.

In the second round of interviews, we asked each of the managers for details about the PHI leak detection and mitigation process: (1) How was the inadvertent disclosure identified? (2) Was it detected before or after the event? (3) What was done to fix it? (4) What could have been done to fix it (but was not)? (5) Other details of the setting?

In some cases, the managers were not aware of the details of the PHI leaks. In those cases, they asked for additional time to seek clarification from other employees in the organization. The details of the PHI leaks obtained from the interviews provided a

[8] For brevity, we refer to these incidents or scenarios describing the process of inadvertent disclosure as "scenarios" or "incidents."

foundation for evaluating the activity system for the detection and mitigation of PHI leaks. It provided a means to describe the various data access encounters that take place within the healthcare workflow in order to facilitate patient care.

5.2.3 Data Analysis of PHI Leak Scenarios

After the interviews were completed, we obtained several unique scenarios of PHI leaks. In response to leak detection, healthcare managers confirmed that leak detection consists of components of the activity system. For instance, the healthcare manager from Tennessee stated that "tracking every action of the user can provide details on who opened what record at what time in what location." In this scenario, tracking takes place through tools, actions are a part of division of labor, the user is the subject, the record is the object, location hints at community, and time is a type of rule. In the same vein, while analyzing PHI leak mitigation, the healthcare managers confirmed the common categories of activity systems for enforcing user access. For example, the manager from California pointed out that their technology vendors were limited by the security measures of the VPNs, while IT staff had full access to logs and sensitive information. In this scenario,[9] staff members are subjects, logs are objects, VPN is a tool, information technology is the department, and rules include constraints for limiting access.

5.3 Case Application

Participant review was performed on the following PHI leak scenario relayed by the healthcare manager from Tennessee: An employee wanted to convert a data file from an old application. To do this, the employee used an online converter tool and pasted the data file from the old application into the tool. The data file had PHI content in it, and the monitoring systems thus immediately flagged the user for the data breach. The employee was notified of the potential breach and was monitored for a few weeks. The AT-based model allowed us to identify two processes related to this scenario: (1) one in which the employee retrieved the data file from the old application, and (2) one where that employee used a conversion tool to format the data file. In the first process, the employee is the subject in the process and is a part of the hospital community along with other stakeholders. The object is the data file that is retrieved from the old application, which is the tool. In the second process, the employee is still the subject and the data file with PHI content is still the object. However, the community is the internet, and the task of converting the data file is governed by a set of rules—e.g., the file should be free of any PHI content. The employee used the online converter tools to derive the converted file.

In the first process,[10] which utilizes the access request system for leak detection, the information about the employee, the data file, the old application, and the hospital community is identified in the scenario. Since the employee was able to access PHI data from the old application within the hospital community, the privilege set requested by the employee matched the privilege set specified by the patient; thus, the employee was allowed access to a data file from the old application. In the second process, the information about the employee, the data file, the online converter tool, and the internet community are identified in the scenario. In this process, the rules of data exchange (i.e., data files intended for public use should be free of PHI content) are also applicable. Since PHI cannot be released to the online public on the internet, the privilege set requested by the employee did not match the privilege set specified by the organization, and thus a potential PHI leak was detected. The employee was not allowed access to the online converter tool because of a potential PHI leak.

In order to design the enforcement policies for mitigating this PHI leak, the information about the employee, patient data, rules of data exchange, tools for conversion, and the responsibility of the employee are enforced. For example, an employee may be notified about the rule regarding the presence of PHI content when exchanging data with the online community, or it may be recommended that the employee use in-house online converters to perform the conversion or formatting of the data file. Alternatively, the employee may also be advised to seek permission from higher management for such conversions. In this scenario, the employee was reported to upper management and was monitored for a few weeks.

The manager from Tennessee suggested that she could see her organization performing data conversion but believed it would be more likely be done through vendors. She explained that vendors' accounts should be set up using three-step authentication that required a system password, VPN password, and FTP password. Further, she also recommended service-level agreements consisting of access request authorizations, memorandums of partnership, and confidentiality agreements. The PHI leak detection and mitigation model allows these enforcement mechanisms to be implemented. In particular, objects can be desensitized for sensitive data removal, the community can be forced to include approved vendors,

[9] Division of labor is not specified in this example.

[10] The rule that data files intended for public use should be free of PHI content does not apply to this process.

rules can capture the authentication process, responsibility can capture confidentiality and partnership agreements, and tools can account for the website and instruments used for conversion. The manager confirmed that the raw details of the enforcement points within the PHI leak scenario were completely represented by the model. In addition, she also confirmed that the concepts were accurately extracted.

5.4 Transaction Testing

Based on the PHI leak detection and mitigation model (from Figure 4) we discuss the architecture of the process of access control policy matching and access control policy enforcement. As an initial setup, we start with a pool of patients and their data set (Step 1). Once the system is deployed, its first task is to build the privilege set—a defined set of permissions that determines a level of access (Step 2). Privilege sets are generated based on activity theory (consisting of the user roles within the community for requesting the patient data through certain tools that are subject to the rules of request and the responsibility of the requester). The access request system utilizes the privilege set for all the users in the healthcare community.

Each user request is framed in the form of a privilege set (Step 3). This request set is compared with the privilege set to decide whether the rights should be granted. For every action, the request is matched with a privilege set for leak detection (Step 4). For nonmatching results, the policy set for leak mitigation enforces user obligations such as login through VPN channel, security passwords, etc. The privilege set detects the information flow given certain policy specifications. The policy sets are created and deleted based on the current context with every request for patient data. Whenever a request is received, the access response system is used to generate the policy sets (Step 5). Table 9 summarizes the process of PHI leak detection and mitigation, and Figure 6 depicts the related architecture; numbered circles denote each of the five steps.

The primary objective of PHI leak detection and mitigation is to prevent illegal information flow from one point to the other in the activity system. In order to prevent the flow of illegal information, it is important to provide restrictions in the form of enforcement policies. Restrictions are enforced on the client side by executing policies containing rules to permit or deny access to the information. In order to compute the new set of restrictions, all requests that are not a part of the privilege set are added to the illegal information flows. For each illegal information flow, a "deny" restriction is added if the restriction is not already present. Such a restriction prevents the current user from tampering with the patient data and setting liberal rights on the data. Also, when a new patient is enrolled, the privilege sets of all the users are recomputed. When a patient is deleted, the static access rights are checked and, if allowed, data are deleted and the privilege sets of all users are updated.

We summarize the information leak detection and mitigation prototype in a step-by-step manner as follows. We built the prototype system coded in Java programming language to evaluate the proposed framework. This prototype utilizes AT concepts to facilitate leak detection and mitigation. It enables key stakeholders such as physicians, researchers, and other medical staff members to enter patient information and share it with other parties. The prototype system development team consisted of three computer science graduate students and one MIS graduate student with experience in the software industry. The prototype followed the standard software development life cycle (SDLC) methodology and took ten months (two semesters) to complete.

As a prototype, this system developed only a portion of the functionalities required by the actual PHI leak prevention system. These functionalities utilized key constructs such as the practitioner and PHI and their relationships. The prototype system contained four modules including logging, reporting, modularizing, and exporting. There were more than 25 forms generated over six database tables to store relevant construct and relationship information. Figure 7 provides snapshots of the prototype. For the database diagram and use case diagram, see Figure B1 and B2 in Appendix B).

The prototype shows how policies are created around the subject (physician), object (PHI), community (hospital), tool (email), rules (matching), responsibility (administrator), and outcome (access). In Figure 7a, the physician is authorized to read and write patient information (PID # 13) in the hospital. Figure 7b shows the screen when a physician requests patient information (PID # 13). This request is denoted as a transaction (TID # 5). The resulting policy for this request is shown in Figure 7c. Since the physician is authorized for access on PID # 13 or TID # 5, the physician is able to access the patient data as shown in Figure 7d. If the physician tries to access a patient record (for example, PID # 10 or TID # 2) for which he or she is not authorized, it results in a PHI leak. In that case, the rule of mismatch gets executed, and the admin/patient is contacted via email/phone as specified in the setup of the policy in Figure 7a. This PHI leak mitigation is shown in Figure 7e.

Table 9. Process of PHI Leak Detection and Mitigation

1. Admin sets up initial user control on the patient data set
2. This user control builds the privilege set based on AT (subject, object, community, tool, rule, responsibility)
3. On information flow, request is generated in the form (subject, object, community, tool, rule, responsibility)
4. This request is verified against privilege set (from step 2)
5. For mismatch information, policies are generated based on AT (subject, object, community, tool, rule, responsibility)

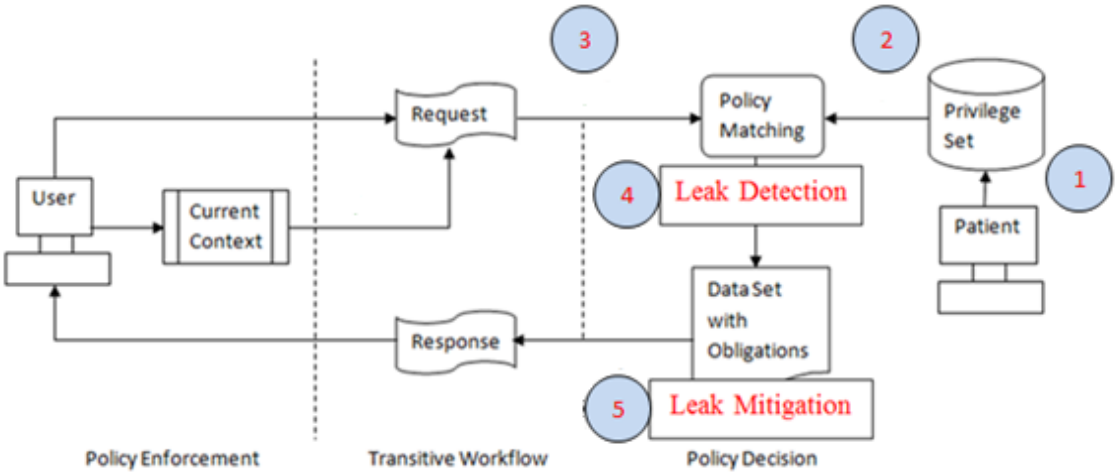


Figure 6. Architecture of Leak Detection and Mitigation

Figure 7a. Policy Setup

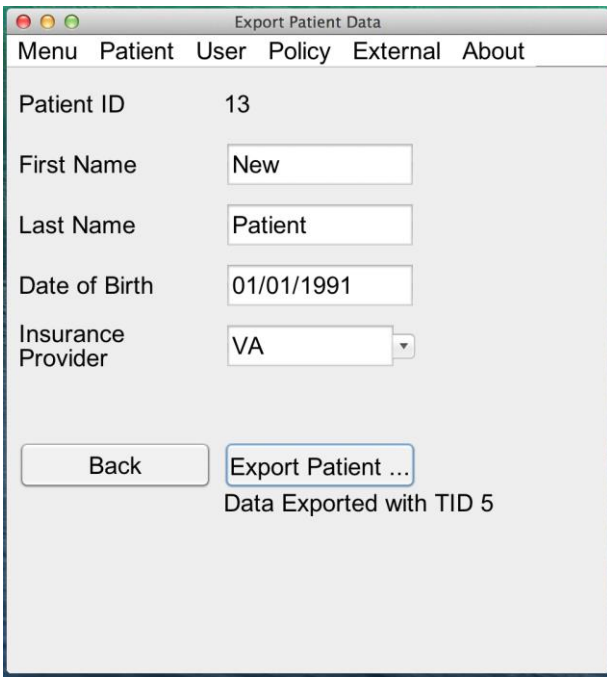


Figure 7b. Patient Data Request

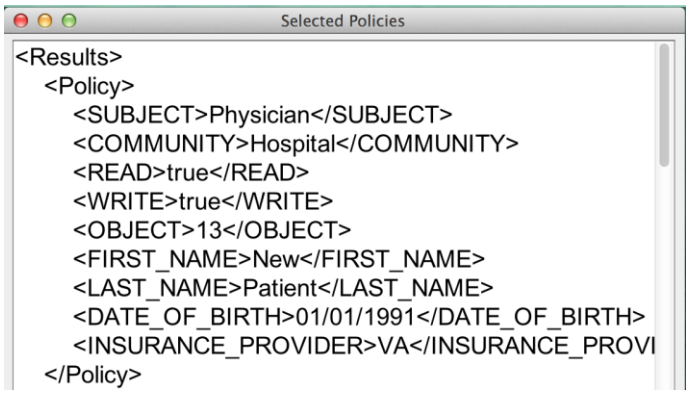


Figure 7c. Policy for Patient Data

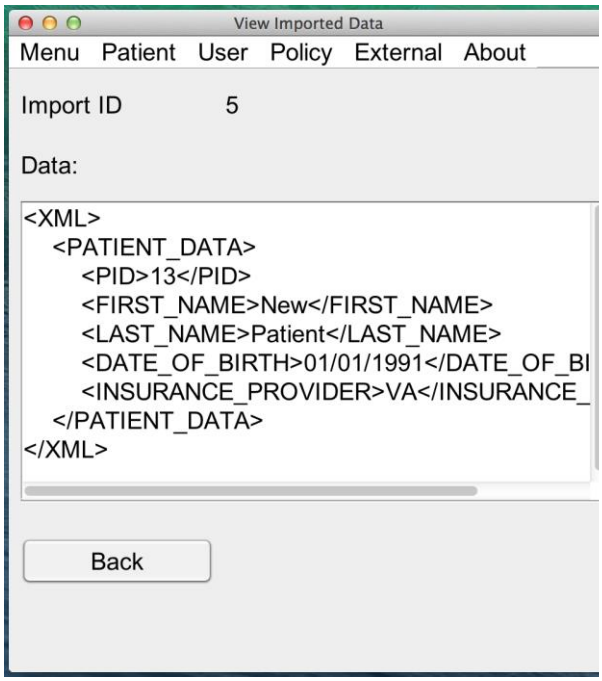


Figure 7d. No PHI Leak (Matched Policy)

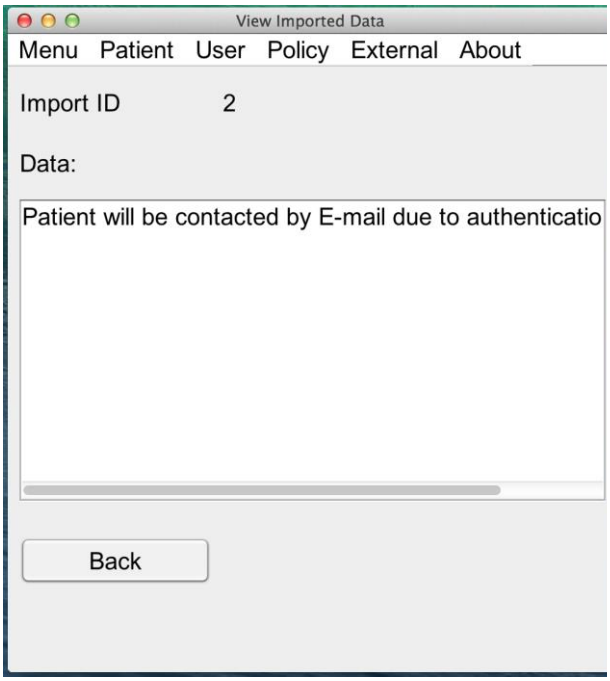


Figure 7e. PHI Leak (Mismatched Policy)

Figure 7. Leak Detection and Mitigation Prototype

6 Discussion and Conclusion

Designing health access control is difficult because of the complexities of healthcare systems (Margheri et al., 2013). Traditional access control models take static elements of the context into account; however, they are not designed to address information leaks. Thus, we argue that leak points should be considered in the design of access control models in the healthcare context for the management of potential healthcare crises. Furthermore, access control models require data classification schemes dealing with sensitive data, data inventory relating to its storage, and data accountability concerning data flows.

The concepts of activity theory (AT) have significant implications for our study. AT can be useful for understanding the various workflow activities (Shankar et al., 2010). AT also enables us to investigate the complex nature of the healthcare workflow by allowing for the study of interactions within the environment that undergo restructuration. We therefore maintain that AT should be utilized as a lens to capture a view of PHI leak detection and mitigation.

Our study makes the following contributions. First, this study analyzes an understudied area of information leakage in the healthcare setting—the detection and mitigation of PHI leakage. The prior literature has emphasized a content-based point of view in detecting and mitigating information leaks. We utilize a contextual view that enables the investigation of information leakages as situated in a meaningful and socially constructed context.

Second, we map access control policy onto an activity system by recognizing the key data elements of the health information flow valued by policy designers. This mapping can enable designers to focus on task-related information within PHI leak scenarios instead of devoting their efforts to the modeling of technical details related to the leak (Kofod-Petersen and Cassens, 2006).

Finally, we examine descriptions of reflective experiences derived from semistructured interviews with four healthcare practitioners for developing a model for detecting and mitigating PHI leaks. This work contributes to the healthcare systems literature in that it (1) recommends the design of an access control model based on AT, (2) adapts AT to propose "request" and "response" systems as interacting activity systems, and (c) develops an access control model for detecting and mitigating PHI leaks within the healthcare context.

This paper has a few limitations. First, we do not consider transitivity within the health organizations. Second, these organizations may have different role hierarchies than assumed here. In addition, the security policies are applied at the user machine and not to the patient information within the entire healthcare workflow. Finally, because of the time constraints of the healthcare managers we consulted, we were unable to pursue the demonstration of our model's utility relative to existing artifacts with them. Future research could explore access control models applicable to various communities.

Acknowledgments

This material is based on work supported by the National Science Foundation under Grant No #2020252. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation. We thank the senior editor and the review team for their critical suggestions that have greatly improved the paper.

References

Allen, D. K., Brown, A., Karanasios, S., and Norman, A. (2013). How should technology-mediated organizational change be explained? A comparison of the contributions of critical realism and activity theory. *MIS Quarterly*, *37*(3), 835-854.

Alneyadi, S., Sithirasenan, E., and Muthukkumarasamy, V. (2016). A survey on data leakage prevention systems. *Journal of Network and Computer Applications, 62,* 137-152.

Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: Current state of research. *International Journal of Internet And Enterprise Management, 6*(4), 279-314.

Ardagna, C. A., Di Vimercati, S. D. C., Foresti, S., Grandison, T. W., Jajodia, S., & Samarati, P. (2010). Access control for smarter healthcare using policy spaces. *Computers and Security, 29*(8), 848-858.

Avital, M., Lyytinen, K. J., Boland Jr, R., Butler, B. S., Dougherty, D., Fineout, M., Jansen, W., Levina, N., Rifkin, W., & Venable, J. (2006). Design with a positive lens: An affirmative approach to designing information and organizations. *Communications of the Association for Information Systems, 18*, 519-545.

Bertelsen, O. W., & Bødker, S. (2003). Activity theory. In J. M. Carroll (Ed.), HCI Models, Theories, and Frameworks: Toward a Multidisciplinary Science (pp. 192-324). Morgan Kaufmann.

Beznosov, K. (1998). Requirements for access control: US healthcare domain. *Proceedings of the ACM Workshop on Role-Based Access Control*.

Bharosa, N., Lee, J., Janssen, M., & Rao, H. R. (2012). An activity theory analysis of boundary objects in cross-border information systems development for disaster management. *Security Informatics, 1,* Article 15.

Blobel, B. (2004). Authorisation and access control for electronic health record systems. *International Journal of Medical Informatics, 73*(3), 251-257.

Broghammer, M. (2017). Bungled access control spills data on 200 million Americans. Maybe you? *Quest*. https://www.quest.com/community/b/en/posts/bungled-access-control-spills-data-on-200-million-americans-maybe-you

Brossard, D. (2011). Coarse-grained vs. fine-grained access control. *Harvesting Web Technologies.* https://www.webfarmr.eu/2011/05/coarse-grained-vs-fine-grained-access-control-part-i/

Cebul, R. D., Love, T. E., Jain, A. K., & Hebert, C. J. (2011). Electronic health records and quality of diabetes care. *New England Journal of Medicine, 365*(9), 825-833.

Chen, R., Sharman, R., Chakravarti, N., Rao, H. R., & Upadhyaya, S. J. (2008). Emergency response information system interoperability: Development of chemical incident response data model. *Journal of the Association for Information Systems, 9*(3), 200-230.

Chen, R., Sharman, R., Rao, H. R., & Upadhyaya, S. (2013). Data model development for fire related extreme events: An activity theory approach. *MIS Quarterly, 37*(1).

Choi, H., & Kang, M. (2008). Analyzing learner behaviours, conflicting and facilitating factors of online collaborative learning using activity system. *Proceedings of the 2008 International Conference on Learning Sciences*.

Connolly, T., & Begg, C. (2002). *Database systems: A practical approach to design, implementation, and management* (3rd ed). Addison-Wesley.

Damiani, E., De Capitani di Vimercati, S., Paraboschi, S., & Samarati, P. (2002). A fine-grained access control system for XML documents. ACM *Transactions on Information and System Security, 5*(2), 169-202.

Duhbaci, K., & Gupta, M. (2007). *A practical analysis of a collaborative work using activity theory* (Unpublished master's thesis). IT University Kista, Stockholm, Sweden.

Edjlali, G., Acharya, A., & Chaudhary, V. (1998). History-based access control for mobile code. *Proceedings of the 5th ACM Conference on Computer and Communications Security*.

Edwards, B. J. (2009). *It takes a village: Perceptions of the SFU Education research assistant experience* (Unpublished doctoral dissertation). Simon Fraser University, Barnaby: BC, Canada.

El Emam, K., Neri, E., Jonker, E., Sokolova, M., Peyton, L., Neisa, A., & Scassa, T. (2010). The inadvertent disclosure of personal health information through peer-to-peer file sharing programs. *Journal of the American Medical Informatics Association, 17*(2), 148-158.

Engeström, Y. (1987). *Learning by expanding: An activity-theoretical approach to developmental research.* Orienta-Konsultit.

Engeström, Y. (1999). Activity theory and individual and social transformation. In Y. Engeström, Reijo Miettinen, & Raija-leena Punamäki (Eds.), *Perspectives on activity theory* (pp. 19-38). Cambridge University Press.

Engeström, Y. (2000). Activity theory as a framework for analyzing and redesigning work. *Ergonomics, 43*(7), 960-974.

Engeström, Y. (2001). Expansive learning at work: Toward an activity theoretical reconceptualization. Journal of Education and Work, 14(1), 133-156.

Engeström, Y. (2019). Medical work in transition: Towards collaborative and transformative. In A. Bleakly (Ed.) *Routledge handbook of the medical humanities* (pp. 41-54). Routledge.

Falcao-Reis, F., Costa-Pereira, A., & Correia, M. E. (2008). Access and privacy rights using web security standards to increase patient empowerment. *Studies in Health Technology and Informatics, 137*, 275-285.

Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. *Journal of Biomedical Informatics, 46*(3), 541-562.

Ferreira, A., Cruz-Correia, R., Antunes, L. H. M., Farinha, P., Oliveira-Palhares, E., Chadwick, D. W., & Costa-Pereira, A. (2006). How to break access control in a controlled manner. *Proceedings of the 19th IEEE International Symposium on Computer-Based Medical Systems*.

Fuentes, R., Gómez-Sanz, J. J., & Pavón, J. (2004). Social analysis of multi-agent systems with activity theory. In R. Fuentes, J. J. Gómez-Sanz, & J Pavón (Eds.), *Current topics in artificial intelligence* (pp. 526-535). Springer.

Gafny, M. A., Shabtai, A., Rokach, L., & Elovici, Y. (2011). Poster: Applying unsupervised context-based analysis for detecting unauthorized data disclosure. *Proceedings of the 18th ACM Conference on Computer and Communications Security*.

Garg, A. X., Adhikari, N. K., McDonald, H., Rosas-Arellano, M. P., Devereaux, P. J., Beyene, J., Sam, J., & Haynes, R. B. (2005). Effects of Computerized Clinical Decision Support Systems on Practitioner Performance and Patient Outcomes: A Systematic Review. JAMA, *293*(10), 1223-1238.

Goldstein, B. A., Navar, A. M., Pencina, M. J., & Ioannidis, J. (2017). Opportunities and challenges in developing risk prediction models with electronic health records data: a systematic review. *Journal of the American Medical Informatics Association, 24*(1), 198-208.

Harel, A., Shabtai, A., Rokach, L., & Elovici, Y. (2010). M-score: Estimating the potential damage of data leakage incident by assigning misuseability weight. *Proceedings of the 2010 ACM workshop on Insider Threats*.

Harel, A., Shabtai, A., Rokach, L., & Elovici Y. (2012). M-Score: A misuseability weight measure. *IEEE Transactions on Dependable and Secure* Computing*, 9*(3): 414-428.

Hasan, H., & Banna, S. (2012). The unit of analysis in IS theory: The case for activity. In D. Hart, & S. Gregor (Eds.), *Information Systems Foundations: Theory building in information systems* (pp. 191-214). ANU Press.

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

Ho, S. M., Hancock, J. T., Booth, C., & Liu, X. (2016). Computer-mediated deception: strategies revealed by language-action cues in spontaneous communication. *Journal of Management Information Systems, 33*(2), 393-420.

Ho, S. M., & Warkentin, M. (2017). Leader's dilemma game: An experimental design for cyber insider threat research. *Information Systems Frontiers, 19*(2), 377-396.

Hu, J., Peyton, L., & El Emam, K. (2010). A systematic approach to PHI leak prevention in continuous health care data integration. *Proceedings of the Intelligent Methods for Protecting Privacy and Confidentiality in Data Workshop*.

Igira, F. T. (2008). The situatedness of work practices and organizational culture: implications for information systems innovation uptake. *Journal of Information Technology, 23*(2), 79-88.

Islam, S. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. S. (2015). The internet of things for health care: A comprehensive survey. *IEEE Access, 3*, 678-708.

Johnson, M. E. (2009). Data hemorrhages in the health-care sector. In R. Dingledine, P. Golle (Eds.), Financial cryptography and data security (pp. 71-89). Springer.

Johnson, M. E., & Willey, N. D. (2010). Usability failures and healthcare data hemorrhages. *IEEE Security and Privacy*, *2*, 35-42.

Johnson, M. E., & Willey, N. (2011). Will HITECH heal patient data hemorrhages? *Proceedings of the 44th Hawaii International Conference on System Sciences*.

Jonassen, D. H. (2000). Revisiting activity theory as a framework for designing student-centered learning environments. In D.H. Jonassen, & S.M. Land (Eds.), *Theoretical foundations of learning environments* (pp. 89-121). Erlbaum.

Jonassen, D. H., & Rohrer-Murphy, L. (1999). Activity theory as a framework for designing constructivist learning environments. *Educational Technology Research and Development, 47*(1), 61-79.

Kale, S. A., & Kulkarni, S. V. (2012). Data Leakage Detection. *International Journal of Advanced Research in Computer and Communication Engineering, 1*(9), 32-35.

Kaptelinin, V., Kuutti, K., & Bannon, L. (1995). Activity theory: Basic concepts and applications. *Proceedings of the International Confrerence on Human-Computer Interaction* .

Kaptelinin, V., Nardi, B. A., & Macaulay, C. (1999). Methods and tools: The activity checklist: a tool for representing the "space" of context. *Interactions, 6*(4), 27-39.

Karanasios, S., Allen, D., & Finnegan, P. (2015). Call for Papers: Special issue on activity theory in information systems research. *Information Systems Journal, 25*(3), 309-313.

Karanasios, S., Thakker, D., Lau, L., Allen, D., Dimitrova, V., & Norman, A. (2013). Making sense of digital traces: An activity theory driven ontological approach. *Journal of the American Society for Information Science and Technology, 64*(12), 2452-2467.

Katz, G., Elovici, Y., & Shapira, B. (2014). CoBAn: A context based model for data leakage prevention. *Information Sciences, 262*, 137-158.

Kofod-Petersen, A., & Cassens, J. (2006). Using activity theory to model context awareness. In T. R. Roth-Berghofer, S. Schulz, and D. B. Leake (Eds.), *Modeling and retrieval of context* (pp. 1-17). Springer.

Korpela, M., Soriyan, H. A., & Olufokunbi, K. C. (2001). Activity analysis as a method for information systems development. *Scandinavian Journal of Information Systems, 12*(1-2), 191-210.

Kuutti, K. (1996). Activity theory as a potential framework for human-computer interaction research. In *Context and consciousness: Activity theory and human-computer interaction by B.A. Nardi (Ed.)* (pp. 17-44). The MIT Press, Cambridge, MA.

Lechler, T., Wetzel, S., & Jankowski, R. (2011). Identifying and evaluating the threat of transitive information leakage in healthcare systems. *Proceedings of the 44th Hawaii International Conference on System Sciences*.

Leont'ev, A. (1974). The problem of activity in psychology. *Soviet Psychology, 13*(2), 4-33.

Leont'ev, A. (1978). *Activity, consciousness, and personality.* Progress.

Lien, C. C., Ho, C. C., & Tsai, Y. M. (2011). Applying fuzzy decision tree to infer abnormal accessing of insurance customer data. *Proceedings of the Eighth International Conference on Fuzzy Systems and Knowledge Discovery*.

Lovis, C., Spahni, S., Cassoni, N., & Geissbuhler, A. (2007). Comprehensive management of the access to the electronic patient record: towards trans-institutional networks. *International Journal of Medical Informatics, 76*(5), 466-470.

March, S. T., & Scudder, G. D. (2017). Predictive maintenance: strategic use of IT in manufacturing organizations. *Information Systems Frontiers*, *21*(2), 327-341.

Margheri, A., Masi, M., Pugliese, R., & Tiezzi, F. (2013). *A formal software engineering approach to policy-based access control.* http://facpl.sourceforge.net/research/Facpl-TR.pdf

Margheri, A., Masi, M., Pugliese, R., & Tiezzi, F. (2013). On a formal and user-friendly linguistic approach to access control of electronic health data. http://cse.lab.imtlucca.it/~tiezzi/papers/MMPT_healthinf.pdf

Mathew, S., Petropoulos, M., Ngo, H. Q., & Upadhyaya, S. (2010). A data-centric approach to insider attack detection in database systems. *Proceedings of the International Workshop on Recent Advances in Intrusion Detection*.

Milutinovic, S. (2008). The need for the use of XACML access control policy in a distributed EHR and some performance considerations. *Medical and Care Compunetics,* 137, 346-352.

Mohan, A., & Blough, D. M. (2010). An attribute-based authorization policy framework with dynamic conflict resolution. *Proceedings of the 9th Symposium on Identity and Trust on the Internet*.

Motta, G. H., & Furuie, S. S. (2003). A contextual role-based access control authorization model for electronic patient record. *IEEE Transactions on Information Technology in Biomedicine*, 7(3), 202-207.

Mwanza, D. (2001). Where theory meets practice: A case for an activity theory based methodology to guide computer system design. *Proceedings of the Eighth IFIP TC 13 Conference on Human-Computer Interaction*.

Nardi, B. (1995). Activity theory and human-computer interaction. In B. A. Nardi (Ed.), *Context and consciousness: activity theory and human-computer interaction*. MIT Press.

Nita-Rotaru, C., & Li, N. (2004). A framework for role-based access control in group communication systems. *Proceedings of the ISCA 17th International Conference on Parallel and Distributed Computing Systems*.

Papadimitriou, P., & Garcia-Molina, H. (2011). *Data leakage detection. IEEE Transactions on Knowledge and Data Engineering, 23*(1), 51-63.

Park, J., & Ho, S. (2004). Composite role-based monitoring (CRBM) for countering insider threats. In H. Chen, R. Moore, D. D. Zeng, & J. Leavitt J. (Eds.) *Intelligence and security informatics. ISI* 2004 (pp. 201-213). Springer

Parsons, J., & Wand, Y. (1997). Using objects for systems analysis. *Communications of the ACM, 40*(12), 104-110.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems, 24*(3), 45-77.

Peleg, M., Beimel, D., Dori, D., & Denekamp, Y. (2008). Situation-based access control: Privacy management via modeling of patient data access scenarios. *Journal of Biomedical Informatics, 41*(6), 1028-1040.

Raghu, T. S., Jayaraman, B., & Rao, H. R. (2004). Toward an integration of agent-and activity-centric approaches in organizational process modeling: Incorporating incentive mechanisms. *Information Systems Research, 15*(4), 316-335.

Rai, A. (2017). Editor's comments: Diversity of design science research. *MIS Quarterly, 41*(1), iii-xviii.

Rees, J., & Barkhi, R. (2001). The problem of highly constrained tasks in group decision support systems. *European Journal of Operational Research, 135*(1), 220-229.

Rosemann, M., Recker, J., & Flender, C. (2008). Contextualisation of business processes. International Journal of Business Process Integration and Management, 3(1), 47-60.

Rostad, L. (2008). An initial model and a discussion of access control in patient controlled health records. In Availability, Reliability and Security, 2008. ARES 08. Third International Conference on (pp. 935-942). IEEE.

Rostad, L., & Edsberg, O. (2006). A study of access control requirements for healthcare systems based on audit trails from access logs. In Computer Security Applications Conference, 2006. ACSAC'06. 22nd Annual (pp. 175-186). IEEE.

Russell, D. R. (2009). Uses of activity theory in written communication research. In *Learning and Expanding with Activity Theory* (pp. 40-52).

Samarati, P., & de Vimercati, S. C. (2000). Access control: Policies, models, and mechanisms. In R. Focardi & R. Gorrieri (Eds.) *Foundations of security analysis and design. FOSAD 2000.* (pp. 137-196). Springer.

Samouilova, M. A. (2005). *Exploring the screenplay writing process: implications for instructional design and cultural-historical activity theory* (Unpublished doctoral dissertation). Pennsylvania State University, University Park, PA.

Sandhu, R., Coyne, E., Feinstein, H., & Youman, C. (1996). Role-based access control models. *Computer, 29*(2), 38-47.

Sandhu, R. S., & Samarati, P. (1994). Access control: principle and practice. *IEEE Communications Magazine, 32*(9), 40-48.

Sannino, A., Daniels, H., & Gutiérrez, K. D. (Eds.). (2009). *Learning and expanding with activity theory.* Cambridge University Press.

Schapranow, M. P. (2012). *Real-time security extensions for EPCglobal networks* (Unpublished doctoral dissertation). Hasso Plattner Institute, University of Potsdam, Potsdam, Germany.

Shankar, D., Agrawal, M., & Rao, H. R. (2010). Emergency response to Mumbai terror attacks: An activity theory analysis. In R. Santanam, M. Sethumadhavan, & M. Virendra (Eds.), *Cyber security, cyber crime and cyber forensics: Applications and perspectives* (pp. 46-58). IGI Global.

Shabtai, A., Elovici, Y., & Rokach, L. (2012). *A survey of data leakage detection and prevention solutions.* Springer.

Smari, W. W., Clemente, P., & Lalande, J. F. (2014). An extended attribute based access control model with trust and privacy: Application to a collaborative crisis management system. *Future Generation Computer Systems, 31*, 147-168.

Sokolova, M., El Emam, K., Arbuckle, L., Neri, E., Rose, S., & Jonker, E. (2012). P2P watch: personal health information detection in peer-to-peer file-sharing networks. *Journal of Medical Internet Research, 14*(4), e95.

Sokolova, M., El Emam, K., Rose, S., Chowdhury, S., Neri, E., Jonker, E., & Peyton, L. (2009). Personal health information leak prevention in heterogeneous texts. *Proceedings of the Association for Computational Linguistics Workshop on Adaptation of Language Resources and Technology to New Domains*.

Soumya, S. R., & Smitha, E. S. (2014). Data leakage prevention system by context based keyword matching and encrypted data detection. *International Journal of Advanced Research in Computer Science Engineering and Information Technology, 3*(1), http://www.isrjournals.org/journals/computerscience_information_technology_journals/dataleakagepreventionsystembycontextbasedkeywordmatchingandencrypteddatadetection1403783875.pdf

Tran, T., Valecha, R., Rad, P., & Rao, H. R. (2019). Misinformation harms during crises: When the human and machine loops interact. *Proceedings of the* I*EEE International Conference on Big Data* (pp. 4644-4646).

Tran, T., Valecha, R., Rad, P., & Rao, H. R. (2020). Misinformation in crises: A conceptual framework for examining human-machine interactions. *Proceedings of the* IEEE/ITU International Conference on Artificial Intelligence for Good (pp. 46-50).

Tremblay, M. C., VanderMeer, D., Rothenberger, M., Gupta, A., & Yoon, V. (Eds.). (2014). Advancing the impact of design science: moving from theory to practice. *Proceedings of the 9th International DESRIST Conference*.

Valecha, R., Kashyap, M., Rajeev, S., Rao, R., & Upadhyaya, S. (2014). An activity theory approach to specification of access control policies in transitive health workflows. *Proceedings of the International Conference on Information Systems.*

Valecha, R., Rao, H. R., Upadhyaya, S. J., & Sharman, R. (2019). An activity theory approach to modeling dispatch-mediated emergency response. *Journal of the Association for Information Systems, 20*(1), 33-57.

Valecha, R., Upadhyaya, S., Rao, R., & Keepanasseril, A. (2012). An activity theory approach to leak detection and mitigation in personal health information (PHI). *Proceedings of the Workshop on Information Security and Privacy.*

Van der Haak, M., Wolff, A. C., Brandner, R., Drings, P., Wannenmacher, M., & Wetter, T. (2003). Data security and protection in cross-institutional electronic patient records. *International Journal of Medical Informatics*, *70*(2), 117-130.

Volkoff, O., Strong, D. M., & Elmes, M. B. (2007). Technological embeddedness and organizational change. *Organization Science, 18*(5), 832-848.

Vygotsky, L.S. (1978). *Mind and society.* Harvard University Press.

Wand, Y., Monarchi, D. E., Parsons, J., & Woo, C. C. (1995). Theoretical foundations for conceptual modelling in information systems development. *Decision Support Systems, 15*(4), 285-304.

Wand, Y., & Weber, R. (2002). Research commentary: Information systems and conceptual modeling—a research agenda. *Information Systems Research, 13*(4), 363-376.

Welch, C. A. (2001). Sacred secrets: The privacy of medical records. *The New England Journal of Medicine, 345*(5), 371-372.

Wilson, E. (2004). Using activity theory as a lens to analyse interaction in a university-school initial teacher education and training partnership. *Educational Action Research, 12*(4), 587-612.

Wimmer, H., Yoon, V. Y., & Sugumaran, V. (2016). A multi-agent system to support evidence based medicine and clinical decision making via data sharing and data privacy. *Decision Support Systems, 88*, 51-66.

Appendix A: Access Control Reports

RACF/ID LAN Request
Add/Change/Delete

Date _____ LAN Liaison/ Sys Adm. _____
Phone Number: _____

Add ☒ Change ☐ (name/access change only) Delete ☐ Current RACF _____

Employees starting in new program area MUST get a new RACF/ID

Request for State Employee ☐ Contract Employee ☐

Regional Employee ☒ County: _____
or
Local Employee ☐ Program Area: _____
(Ex: BMF, CEDS, PPA, VR, COM, WIC

Office User Only **RACF/ID:** _____
Context: _____

Employee Name: _____
Last First M.
Email Address _____
SSN: _____ Effective Date: _____

Employee Phone #: _____ Fax: _____

Address: _____
Floor Bldg Street City Zip

Division: _____ Fiscal Officer Signature _____

Allotment code: _____ Cost Center: _____ Speed Chart _____

Establish User Accounts: NDS/GroupWise ☐ TN3270 ☐ RBS ☐

Authorized AS400 use by: _____

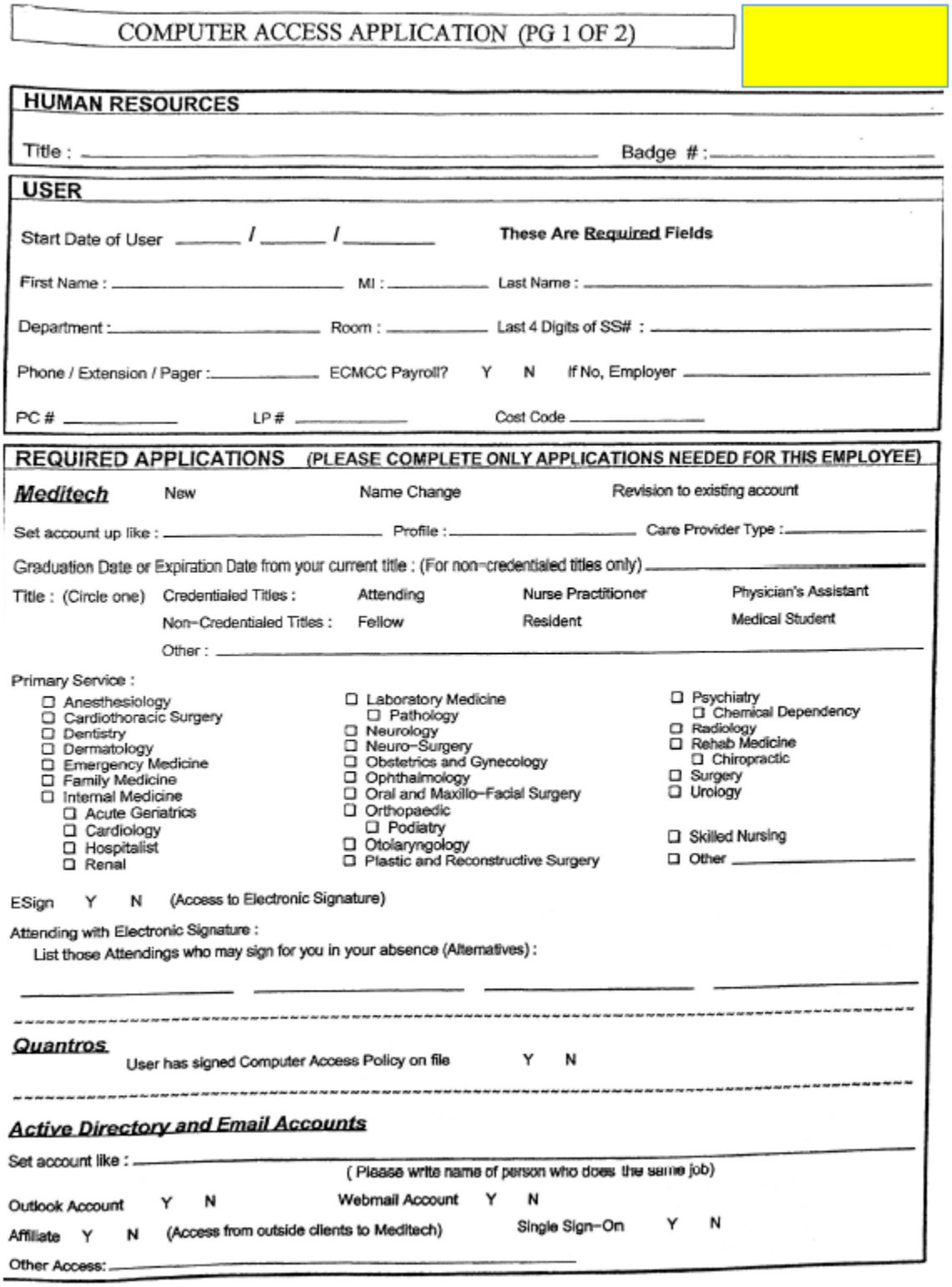
Please Grant Group Membership(s) (specify content of group and access level)
List groups for _____

VPN ACCOUNT METRO to access STD*MIS .
The Employee has signed the Acceptable Use Policy as indicated ☒

Fax to: _____ or Email to: _____

PH3743 Revised. 07/09 **RDA S836-1**

Figure A1. Access Request Reports from Tennessee Health Organization



COMPUTER ACCESS APPLICATION (PG 1 OF 2)

HUMAN RESOURCES

Title : _____ Badge # : _____

USER

Start Date of User ____ / ____ / ____ **These Are Required Fields**

First Name : _____ MI : _____ Last Name : _____

Department : _____ Room : _____ Last 4 Digits of SS# : _____

Phone / Extension / Pager : _____ ECMCC Payroll? Y N If No, Employer _____

PC # _____ LP # _____ Cost Code _____

REQUIRED APPLICATIONS (PLEASE COMPLETE ONLY APPLICATIONS NEEDED FOR THIS EMPLOYEE)

Meditech New Name Change Revision to existing account

Set account up like : _____ Profile : _____ Care Provider Type : _____

Graduation Date or Expiration Date from your current title : (For non-credentialed titles only) _____

Title : (Circle one) Credentialed Titles : Attending Nurse Practitioner Physician's Assistant

Non-Credentialed Titles : Fellow Resident Medical Student

Other : _____

Primary Service :

- ☐ Anesthesiology
- ☐ Cardiothoracic Surgery
- ☐ Dentistry
- ☐ Dermatology
- ☐ Emergency Medicine
- ☐ Family Medicine
- ☐ Internal Medicine
  - ☐ Acute Geriatrics
  - ☐ Cardiology
  - ☐ Hospitalist
  - ☐ Renal
- ☐ Laboratory Medicine
  - ☐ Pathology
- ☐ Neurology
- ☐ Neuro-Surgery
- ☐ Obstetrics and Gynecology
- ☐ Ophthalmology
- ☐ Oral and Maxillo-Facial Surgery
- ☐ Orthopaedic
  - ☐ Podiatry
- ☐ Otolaryngology
- ☐ Plastic and Reconstructive Surgery
- ☐ Psychiatry
  - ☐ Chemical Dependency
- ☐ Radiology
- ☐ Rehab Medicine
  - ☐ Chiropractic
- ☐ Surgery
- ☐ Urology
- ☐ Skilled Nursing
- ☐ Other _____

ESign Y N (Access to Electronic Signature)

Attending with Electronic Signature :

List those Attendings who may sign for you in your absence (Alternatives) :

_____ _____ _____ _____

Quantros

User has signed Computer Access Policy on file Y N

Active Directory and Email Accounts

Set account like : _____

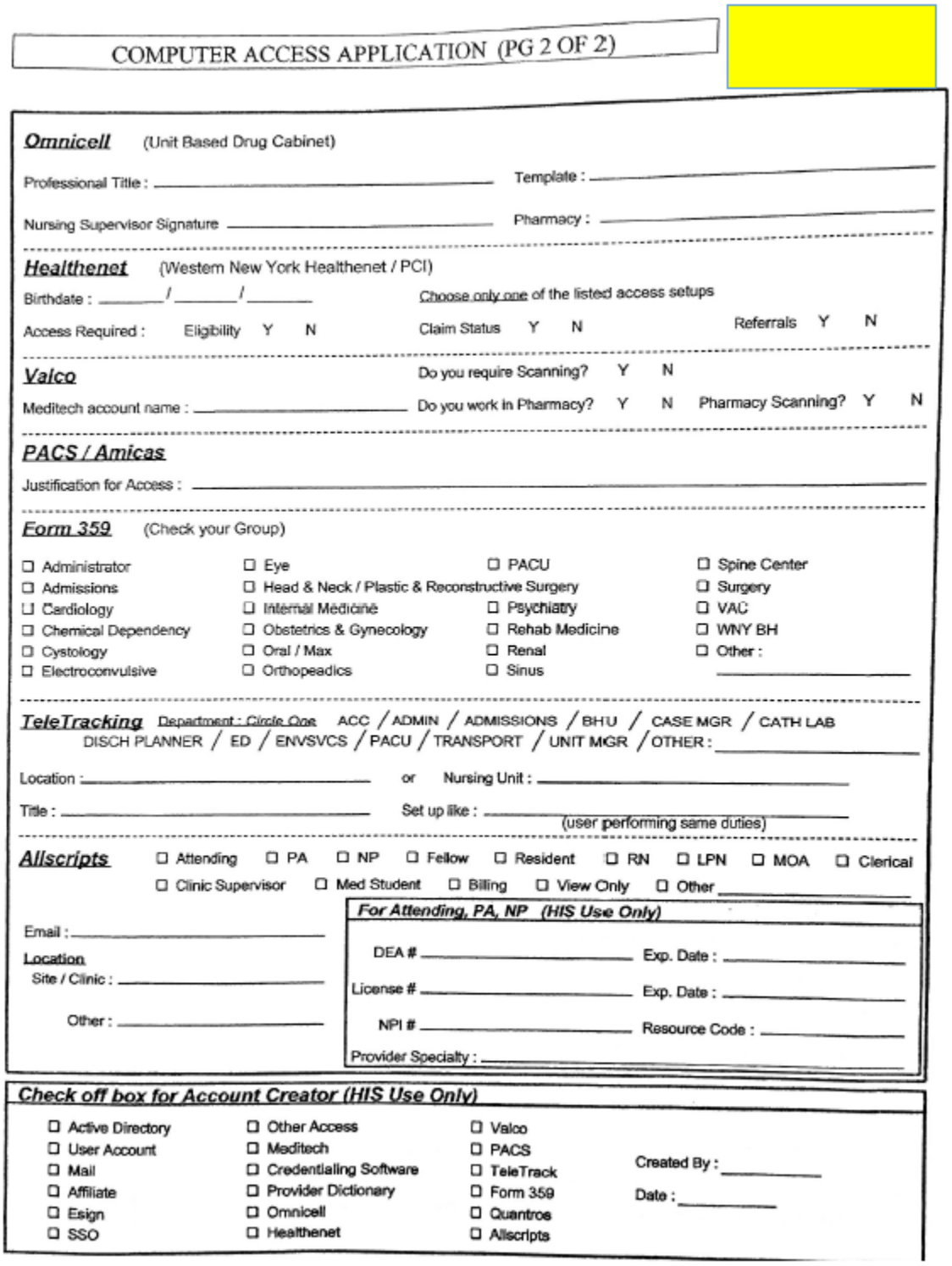
(Please write name of person who does the same job)

Outlook Account Y N Webmail Account Y N

Affiliate Y N (Access from outside clients to Meditech) Single Sign-On Y N

Other Access: _____

Figure A2. Access Request Reports from New York Health Organization (Page 1)



COMPUTER ACCESS APPLICATION (PG 2 OF 2)

Omnicell (Unit Based Drug Cabinet)

Professional Title : _____ Template : _____

Nursing Supervisor Signature _____ Pharmacy : _____

Healthenet (Western New York Healthenet / PCI)

Birthdate : ____/____/____ Choose only one of the listed access setups

Access Required : Eligibility Y N Claim Status Y N Referrals Y N

Valco

Do you require Scanning? Y N

Meditech account name : _____ Do you work in Pharmacy? Y N Pharmacy Scanning? Y N

PACS / Amicas

Justification for Access : _____

Form 359 (Check your Group)

- ☐ Administrator
- ☐ Admissions
- ☐ Cardiology
- ☐ Chemical Dependency
- ☐ Cystology
- ☐ Electroconvulsive
- ☐ Eye
- ☐ Head & Neck / Plastic & Reconstructive Surgery
- ☐ Internal Medicine
- ☐ Obstetrics & Gynecology
- ☐ Oral / Max
- ☐ Orthopeadics
- ☐ PACU
- ☐ Psychiatry
- ☐ Rehab Medicine
- ☐ Renal
- ☐ Sinus
- ☐ Spine Center
- ☐ Surgery
- ☐ VAC
- ☐ WNY BH
- ☐ Other : _____

TeleTracking Department : Circle One ACC / ADMIN / ADMISSIONS / BHU / CASE MGR / CATH LAB DISCH PLANNER / ED / ENVSVCS / PACU / TRANSPORT / UNIT MGR / OTHER : _____

Location : _____ or Nursing Unit : _____

Title : _____ Set up like : _____ (user performing same duties)

Allscripts ☐ Attending ☐ PA ☐ NP ☐ Fellow ☐ Resident ☐ RN ☐ LPN ☐ MOA ☐ Clerical ☐ Clinic Supervisor ☐ Med Student ☐ Billing ☐ View Only ☐ Other _____

Email : _____

Location

Site / Clinic : _____

Other : _____

For Attending, PA, NP (HIS Use Only)

DEA # _____ Exp. Date : _____

License # _____ Exp. Date : _____

NPI # _____ Resource Code : _____

Provider Specialty : _____

Check off box for Account Creator (HIS Use Only)

- ☐ Active Directory
- ☐ User Account
- ☐ Mail
- ☐ Affiliate
- ☐ Esign
- ☐ SSO
- ☐ Other Access
- ☐ Meditech
- ☐ Credentialing Software
- ☐ Provider Dictionary
- ☐ Omnicell
- ☐ Healthenet
- ☐ Valco
- ☐ PACS
- ☐ TeleTrack
- ☐ Form 359
- ☐ Quantros
- ☐ Allscripts

Created By : _____

Date : _____

Figure A3. Access Request Reports from New York Health Organization (Page 2)

Appendix B: Instantiation of PHI Leak Detection and Mitigation Model

The database diagram in Figure B1 explains the back-end functionality related to the key constructs and their relationships. It depicts the policy-centric view wherein the policy describes the access of practitioners to PHI in different contexts. The policy table utilizes the AT concepts of subject, object, community, rule, tool, and responsibility for leak detection and leak mitigation. The use case diagram in Figure B2 depicts the cases for the user groups that the system serves.

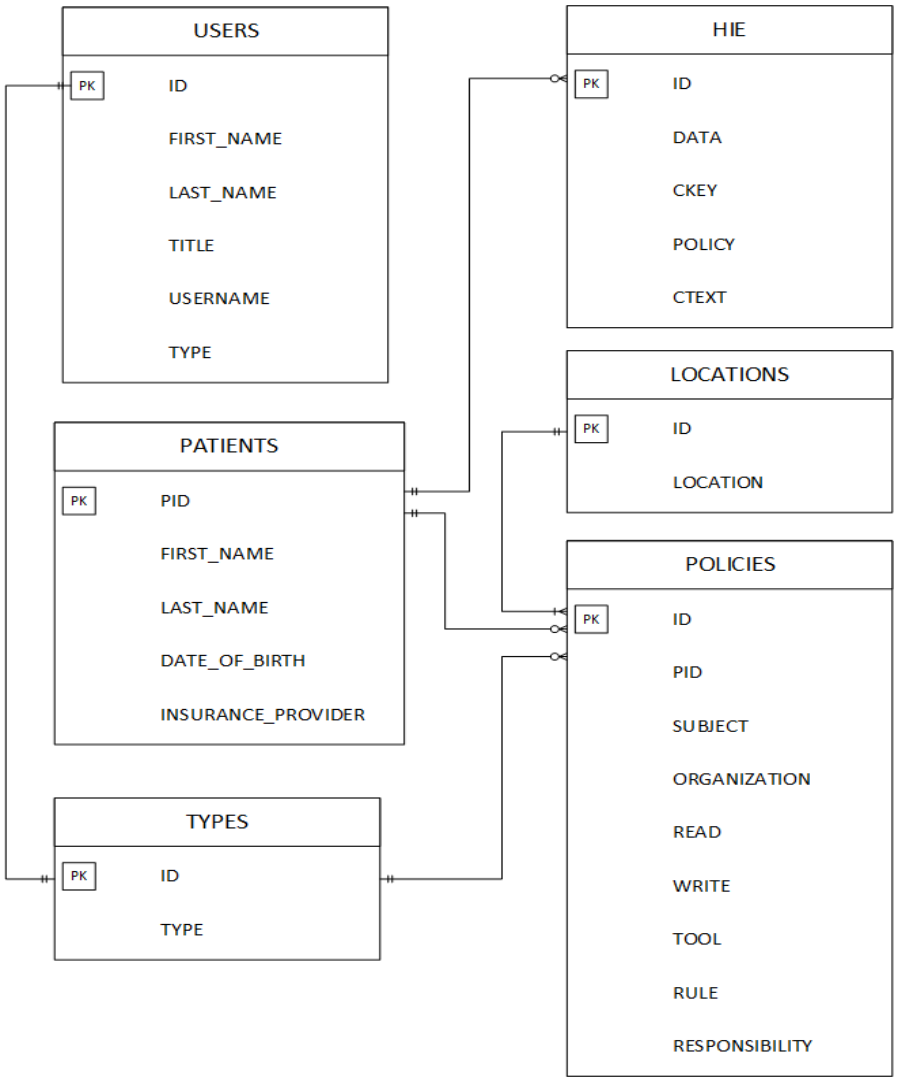


Figure B1. System Database Diagram

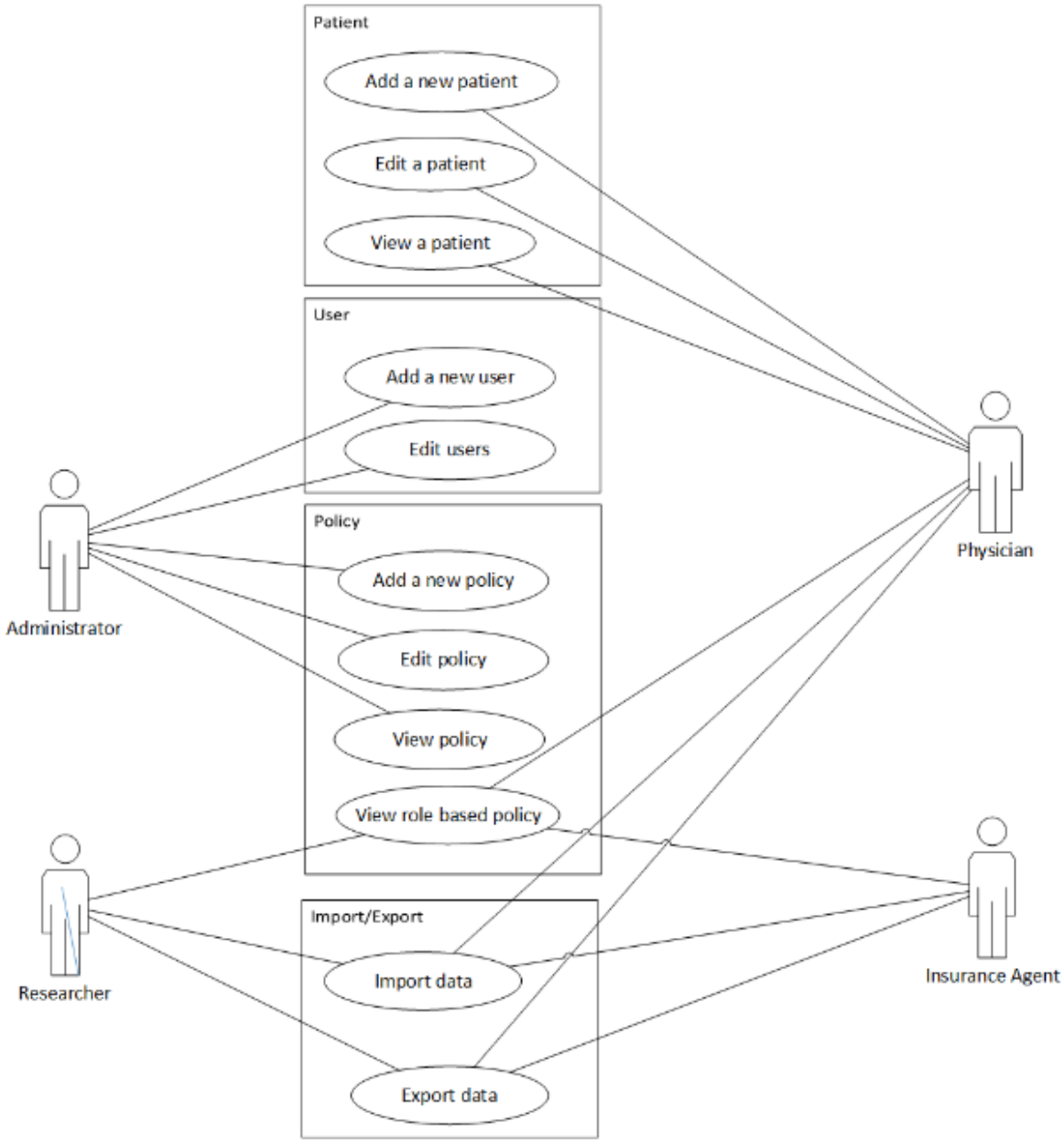


Figure B2. Use Case Diagram

About the Authors

Rohit Valecha is an assistant professor of information systems and cyber security at the University of Texas at San Antonio. He has research interests in the use of social media for crisis response. His research on detection, mitigation, and prevention of misinformation has been funded by NSF. His research has been published in *Management Information Systems Quarterly*, *Journal of the Association for Information Systems*, *Information Systems Frontiers*, *Computers and Security*, *International Journal of Information Management*, and several other ACM and IEEE journals. He received his MS in computer science and PhD in management science and systems from the State University of New York at Buffalo.

Shambhu Upadhyaya is currently a professor of computer science and engineering at the State University of New York at Buffalo, Buffalo, NY, USA, where he also directs the Center of Excellence in Information Systems Assurance Research and Education (CEISARE), designated by the National Security Agency and the Department of Homeland Security. Prior to July 1998, he was a faculty member in the Electrical and Computer Engineering Department. He has authored or coauthored more than 285 articles in refereed journals and conferences in these areas. His research has been supported by the National Science Foundation, US Air Force Research Laboratory, the US Air Force Office of Scientific Research, DARPA, and National Security Agency. His research interests include broad areas of information assurance, computer security, and fault-tolerant computing.

H. Raghav Rao is the AT&T Chair Professor in the Department of Information Systems and Cyber Security, College of Business, University of Texas at San Antonio. He has a courtesy appointment as a professor of computer science. He is currently a Summer Distinguished Visiting Faculty at Swansea University. His interests are in the areas of management information systems, decision support systems, e-business, emergency response management systems and information assurance and artificial intelligence. He has co-edited four books, including *Information Assurance Security and Privacy Services* and *Information Assurance in Financial Services*. He has authored or co-authored more than 200 technical papers, of which more than 125 have been published in archival journals, including *Management Information Systems Quarterly*, *Information Systems Research*, *Journal of Management Information Systems*, and *Journal of the Association for Information Systems*.