Mining Deviations from Patient Care Pathways via Electronic Medical Record System Audits

HE ZHANG, SANJAY MEHOTRA, and DAVID LIEBOVITZ, Northwestern University
CARL A. GUNTER, University of Illinois at Urbana-Champaign
BRADLEY MALIN, Vanderbilt University

In electronic medical record (EMR) systems, administrators often provide EMR users with broad access privileges, which may leave the system vulnerable to misuse and abuse. Given that patient care is based on a coordinated workflow, we hypothesize that care pathways can be represented as the progression of a patient through a system and introduce a strategy to model the patient's flow as a sequence of accesses defined over a graph. Elements in the sequence correspond to features associated with the access transaction (e.g., reason for access). Based on this motivation, we model patterns of patient record usage, which may indicate deviations from care workflows. We evaluate our approach using several months of data from a large academic medical center. Empirical results show that this framework finds a small portion of accesses constitute outliers from such flows. We also observe that the violation patterns deviate for different types of medical services. Analysis of our results suggests greater deviation from normal access patterns by nonclinical users. We simulate anomalies in the context of real accesses to illustrate the efficiency of the proposed method for different medical services. As an illustration of the capabilities of our method, it was observed that the area under the receiver operating characteristic (ROC) curve for the Pediatrics service was found to be 0.9166. The results suggest that our approach is competitive with, and often better than, the existing state-of-the-art in its outlier detection performance. At the same time, our method is more efficient, by orders of magnitude, than previous approaches, allowing for detection of thousands of accesses in seconds.

Categories and Subject Descriptors: J.3 [**Life and Medical Sciences**]: *Medical information systems*

General Terms: Algorithms, Measurement, Security

Additional Key Words and Phrases: Anomaly detection, audit, data mining, graph-based analysis, electronic medical record systems, temporal systems

ACM Reference Format:
Zhang, H., Mehotra, S., Liebovitz, D., Gunter, C. A., and Malin, B. 2013. Mining deviations from patient care pathways via electronic medical record system audits. *ACM Trans. Manage. Inf. Syst.* 4, 4, Article 17 (December 2013), 20 pages.
DOI:http://dx.doi.org/10.1145/2544102

1. INTRODUCTION

Electronic medical record (EMR) systems provide a convenient way for physicians and clinical service providers to interact with, reason over, and contribute to patients' health data [Buntin et al. 2010; Ludwick and Doucette 2009]. EMRs are designed to enable effective [Pizziferri et al. 2005] and safe [Chaudhry et al. 2006] healthcare

This work is supported by the National Institutes of Health, under grant R01-LM010207, the National Science Foundation, under grant CCF-0424422 and grant CNS-0964063, and the Office of the National Coordinator for Health IT, under grant HHS-90TR0003/01.
Author's address: B. Malin; email: b.maln@vanderbilt.edu.

DOI:http://dx.doi.org/10.1145/2544102

practices. However, healthcare organizations (HCOs) are inherently complex and dynamic environments [Bosch et al. 2009; Kannampallil et al. 2011], which makes it difficult for administrators to define access control policies [Malin et al. 2011]. EMR user privileges are therefore often defined at a coarse level to minimize workflow inefficiencies and maximize flexibility in the management of a patient. The consequence of such decisions is that EMR systems are left vulnerable to misuse and, potentially, abuse, from insiders (authenticated employees of the institution), which ultimately can compromise patient confidentiality.

Thus, it is critical to complement access control mechanisms in EMRs with intelligent auditing strategies. Manual review of the access logs of patient records, particularly for public figures, can identify misuse [Gallagher et al. 1998; Zhou and Liu 2005], but such a practice does not scale for surveillance of all medical records in a large HCO. This is because the number of medical records accessed on a daily basis is significantly greater than the time administrative staff have available to perform follow-up investigations. Thus, there has been an increasing focus on the development of data-driven methodologies to support the automated discovery of potentially suspicious accesses with respect to EMR system usage. As we review in the following section in greater detail, auditing strategies have considered ways to winnow the set of access logs using various methods, ranging from heuristic rules (e.g., high volume users [Asaro and Ries 2001]) to sophisticated machine learning classifiers (e.g., support vector machines [Boxwala et al. 2011; Menon et al. 2013]). Nonetheless, the approaches developed to date have mainly focused on a static view of healthcare operations—these approaches tend to neglect the temporal component of patient care.

As a result, the current array of approaches fails to account for the fact that the degree to which a particular access appears suspicious may be inferred from what happened before, as well as after, the event in question. While care pathways are expected [Campbell et al. 1998], they may be difficult to detect or represent for a particular patient, particularly when auditing post hoc. This is because the flexibility and complexity of HCOs may obscure even strong patterns of care. Thus, rather than detect and represent patterns explicitly (which has been done for temporal policy modeling [Peleg et al. 2008]), we believe it may be more scalable to model accesses to a patient's record over time (the sequence of users and affiliated contextual information) to determine when a particular access has significantly deviated from typical practice.

In this article, we establish a patient-flow-based anomaly detection (PFAD) framework using historical access logs from EMRs. In doing so, we aim to establish a scoring model that assesses the degree to which an access can be characterized to have deviated from past patterns within a series of events associated with a patient record. PFAD uses a graph-based model of accesses that captures the ordered relationship between various components of an EMR user's interaction with a patient record, such as the role of the user, their stated reason for accessing the record, or where the patient was located in the healthcare facility. To demonstrate the feasibility of our approach, we investigated the properties of such graphs and deviation scores using several months of access logs from Northwestern Memorial Hospital. Our empirical results suggest that the proposed framework can identify a small proportion of accesses with high deviation scores. Our results also suggest that a small number of access reasons contribute the majority of the deviation scores and that the deviation from access patterns varies with the type of service. We provide results from two different randomized experimental setups and compare PFAD with a competing approach that is considered to be state-of-the-art, to show that our method can detect deviations efficiently.

2. BACKGROUND

As health information technology (HIT) and the healthcare workforce grow in diversity, so too does their complexity. This is a concern because evidence suggests that complex HIT can interrupt care delivery [Ash et al. 2004; Goldschmidt 2005], contribute to medical errors [Campbell et al. 2006], and expose patient data to breaches [King et al. 2012]. Moreover, such events tend to be discovered after they have transpired en masse, leading to undesirable media coverage, loss of patients' trust, and sanctions imposed by state and federal agencies. It is therefore critical that information systems in the healthcare setting are implemented and deployed in a manner that upholds the privacy of the patients to whom the information corresponds.

A substantial amount of attention has been allotted to avert hacking from adversaries external to the HCO (e.g., Appari and Johnson [2011], Bansal et al. [2010], Davis and Having [2006], Kwon and Johnson [2013], and Smith and Eloff [1999]). Yet, the insider threat has received less attention from the research community, despite its acknowledgment as a real and growing problem [Manos 2012]. This is a significant concern because evidence suggests the greatest risk to information systems stems from authorized users [Probst et al. 2007; Schultz 2002; Stolfo et al. 2008]. Unchecked access to health information could lead to privacy compromise, deterioration of trust, and eventually harm [Amatayakul 2009; Dimick 2010]. Physicians have also voiced major concerns over the security and confidentiality of current EMR systems [Loomis et al. 2002]. It has been suggested that the safety of EMR systems could be improved by incorporating more stringent security procedures, such as access limitations and detailed audit trails [Goldberg 2000]. In this section, we review the extent to which such procedures have been applied, with a particular focus on insider threat modeling, auditing, and anomaly detection.

2.1. Access Control and Intrusion Detection

It has been suggested that insider threats to EMRs can be addressed via traditional information security practices [Blobel 2004; Sandhu and Samarati 1994; Schoenberg and Safran 2000], such as variations on access control (e.g., role-based [Lee and Chang 2012; Park et al. 2001; Sandhu et al. 1996; Zhang et al. 2003], situation-based [Motta and Furuie 2003; Peleg et al. 2008], and team-based [Georgiadis et al. 2002; Motta and Furuie 2003; Le et al. 2012]). While many commercial EMR systems incorporate such technologies, users are often permitted to "break the glass" to ensure patient care is not disrupted [Ferreira et al. 2006; Marinovic et al. 2011]. The expectation is that broken glass events will be reviewed by administrators, which is possible when the number of escalations is small. One study in Norway, for instance, provides a compelling illustration of how this framework can fail [Rostad and Nytro 2006]. In one month, 50% of approximately 100,000 patients' records were accessed via break-the-glass by 45% of approximately 12,000 users, leading to over 290,000 incidents, which corresponded to around 17% of all accesses. This is clearly a caseload greater than any EMR administrator or healthcare privacy official can handle. Thus, rather than clamp down on access, HCOs often provide broad rights to their employees with the threat of penalties to anyone found to misuse the system. We wish to stress that this does not imply HCOs forgo access controls entirely (e.g., nonclinical staff are not allocated rights to issue medication orders), but rather that read capabilities are often granted liberally.

To mitigate the deficiencies of access control in practice, an emerging paradigm is to extend traditional access control through experience-based access management (EBAM) [Gunter et al. 2011]. The premise of EBAM is to evolve access control systems to reflect the behavior observed in the system. One way to realize EBAM is to mine patterns of appropriate accesses, update the system based on such patterns, and refer an access to system administrators when patterns are violated. The discovered patterns will be updated based on feedback. Along these lines, Bhatti and Grandison [2007] proposed a method to extend and refine privacy policies in the form of logical rules based on patterns mined from access logs. However, this method was not evaluated with actual EMR access log data. More recently, Zhang et al. [2011] have shown that EMR role specifications could be refined using a classification strategy. This approach leverages the attributes associated with accesses (e.g., patient's location in a hospital) to build classifiers for each role. When specific users fail to be classified into their respective roles, the system can relabel the users with a more generalized section of an organizational hierarchy (e.g., *Occupational Therapists* and *Physical Therapists*, may be relabeled as *Rehabilitation Therapists*) to enable a more accurate classifier. While these approaches were designed to enable refinement of polices, they are not necessarily appropriate for the detection of outliers. For instance, the empirical findings from Zhang et al. [2011] illustrated that prediction of a user's role was 50–70% accurate on average.

2.2. Auditing and Anomaly Detection in EMRs

Given the limits of access control, it is important to develop meaningful and scalable intrusion detection strategies. An effective intrusion detection system should not only improve detection, but also lead to increased deterrence for inside users [Cavusoglu et al. 2005]. Various techniques for intrusion detection have been developed and have been assessed in a wide range of application domains (e.g., Chen et al. [2005], Chou et al. [2007], Holton [2009], and Ye et al. [2001]). With respect to the access logs of EMR systems, intrusion detection has been split into rule-based and machine learning-based strategies. Simple rules-based approaches were first introduced in the 1990s, when hospital IT administrators began to inspect the distribution of medical records accessed by users [Asaro and Ries 2001]. It was posited that high-volume users (e.g., employees accessing more than 200 records in a day) may be stepping beyond the boundaries of their role. Recently rules-based approaches have become more intelligent and attempt to explain accesses to medical records [Fabbri and LeFevre 2011, 2013]. Under this model, legitimate accesses to EMRs are associated with a clinical or operational reason specified either explicitly (e.g., "follow-up visit") or implicitly (e.g., an upload of a progress report). This approach can triage a large number of accesses, but there remain a significant proportion unaffiliated with any documentation. Moreover, even when there is documentation, it is not necessarily apparent how an access relates to a broader care process.

To overcome the rigid nature of rule-based systems, machine learning strategies have been developed to search for patterns and detect deviations from such patterns. Machine learning approaches themselves have two subclasses: supervised and unsupervised strategies. The set of strategies, based on supervised approaches, is tuned to detect suspicious accesses based on the knowledge of real intrusions supplied by healthcare officials [Boxwala et al. 2011; Kim et al. 2011; Menon et al. 2013]. Empirical analysis with incidents at several large healthcare providers in Boston demonstrated that such methods can achieve high discriminatory power using traditional classification models (e.g., logistic regression and support vector machines). We view this class of access analysis as complementary to our own. They model suspicious events as a class in a standard machine learning framework, whereas anomalies are simply events that are outside the normal range of behavior. Additionally, these approaches are challenging to deploy in practice because they (1) require significant adjudication from healthcare experts and (2) assume that all types of suspicious activities are known a priori. As an alternative, a second set of automated learning strategies uses unsupervised methods. These approaches use the patterns observed in the system as a model by which deviations can be assessed. Such approaches have been used to model deviations from workflows in intrasession actions Li et al. [2012] (the pattern of a single user interacting with the EMR) and inferred social networks of collaborations across sessions [Chen and Malin 2011; Chen et al. 2012a, 2012b] (pattern of multiple users coordinating to treat a patient). Of most revelevence to our own work, the specialized network anomaly detection model (SNAD) uses a relational analysis of care providers [Chen and Malin 2011] and has been shown to achieve high fidelity in certain EMRs, but it is limited in that it neglects ordered pathways.

2.3. Temporal Anomaly Detection

Beyond EMR systems, we will point out there are several anomaly detection techniques that invoke temporal data mining. Jakkula and Cook [2008] and Jakkula et al. [2008] applied temporal logic to calculate the probability that an event is an anomaly in a smart home environment. Sun et al. [2006] treated the data for one particular timepoint as a tensor, analyzed the principal components of a sequence of tensors, and compared the errors between the observed and predicted tensors to measure the abnormality. Lane and Brodley [1999] divided a sequence into equal length subsequences. They compared the similarity and then measured the irregularity of these subsequences. Our model, based upon a similar idea, aims to discover the temporal patterns and measure the inconsistency between the learned patterns and new data. However, our work is different in that it focuses on the one-step transition in each sequence.

3. METHODS

In this section, we introduce an approach to building a graph-based model that represents the series of EMR accesses resulting from intended activities related to patient care. We refer to this approach as patient flow-based anomaly detection (PFAD).

3.1. A Graph-based Approach for Care Pathway Modeling

To formalize the problem, let $\mathscr{R} := \{r_1, r_2, \ldots, r_{K_r}\}$ be the set of values of a given attribute R and $\mathscr{P} := \{p_1, p_2, \ldots, p_{K_p}\}$ be the set of patients. Attributes can correspond to any property that can be used to test the regularity of an access, including an HCO employee's role, the service a patient is on, the location in the HCO of the patient, or the reason specified for an access. We use (p, r) to define an access to patient p with value r.

For each patient $p \in \mathscr{P}$, the access logs are represented as an ordered sequence (according to the timestamps) of attribute R values as $r_{i_1^p}, r_{i_2^p}, \ldots, r_{i_{N_p}^p}$. Let $G = (V, E)$ be a weighted graph such that $V = \{v_1, \ldots, v_{K_r}\}$ corresponds to vertices for each element in $\mathscr{R}$ and $e_{ij} \in E$ corresponds to an edge between two elements in $\mathscr{R}$. Since the same r may be invoked in adjacent access transactions, we allow self-loops in the graph ($i = j$). Both vertices and edges in the graph will be weighted. Based on this setup, the sequence information for each patient is incorporated into the graph according to the procedure in Algorithm 1.

The basic premise of this algorithm is to count the accesses for each $r \in \mathscr{R}$ and the transitions between accesses for each patient. Figure 1 provides a simple example to illustrate the patient-flow construction algorithm. Imagine there are two patient access sequences defined over the attribute R: $\{\{r_1 \rightarrow r_2 \rightarrow r_4\}, \{r_1 \rightarrow r_2 \rightarrow r_3 \rightarrow r_4\}\}$ and $\mathscr{R} = \{r_1, r_2, r_3, r_4\}$. First, we initialize the graph to consist of four vertices for the corresponding values in $\mathscr{R}$. Next, we follow the procedure in Algorithm 1.

This process begins by instantiating a graph with four nodes (node 1 through node 4) with node and edge weights equal to zero. For the first sequence $r_1 \rightarrow r_2 \rightarrow r_4$, $r_1 \rightarrow$

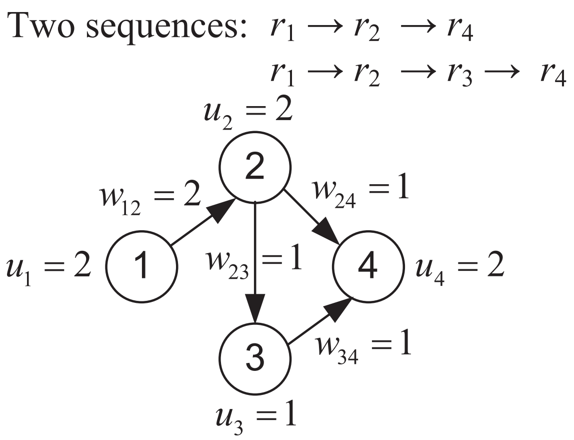

Two sequences: $r_1 \rightarrow r_2 \rightarrow r_4$
$r_1 \rightarrow r_2 \rightarrow r_3 \rightarrow r_4$
$u_2 = 2$
2
$w_{12} = 2$
$w_{24} = 1$
$u_1 = 2$
1
$w_{23} = 1$
4
$u_4 = 2$
3
$w_{34} = 1$
$u_3 = 1$

Fig. 1. An example of patient-flow graph construction for two patients and four reasons.

Algorithm 1 Patient flow graph construction

```
Input: Vectors: An ordered set of attribute $R$ values $[r_{i_1^p}, r_{i_2^p}, \ldots, r_{i_{N_p}^p}]$ for each patient $p \in \mathscr{P}$.
Output: A complete graph $G = V, E$.
Steps:
Let $V = \{v_1, \ldots, v_{K_r}\}$ be the set of attribute $R$ values
Let $G = \{V, E\}$ be a complete graph
Let $U = \{u_1, \ldots, u_{K_r}\}$ be a set of weights for each element of $V$, initially $u_i = 0$ for each i
Let $W = \{w_{11}, \ldots, w_{K_r K_r}\}$ be a set of weights for each pair of elements in $V$, initially $w_{ij} = 0$
  for each $i$, $j$
for each $p \in \mathscr{P}$ do                                ▷ accesses of patient $p$
    for each $j \in \{1, \ldots, N_p - 1\}$ do                   ▷ each access of the patient $p$
        $u_{i_j^p} \leftarrow u_{i_j^p} + 1$                     ▷ increment the weight for $r_{i_1^p}$
        $w_{i_j^p i_{j+1}^p} \leftarrow w_{i_j^p i_{j+1}^p} + 1$   ▷ increment the weight for transition $r_{i_j^p} \rightarrow r_{i_{j+1}^p}$
    end for
end for
$u_{i_j^p} \leftarrow u_{i_j^p} + 1$                             ▷ account for the last vertex of the sequence
return $G$
```

$r_2 \Rightarrow u_1 = 1, w_{12} = 1$, $r_2 \rightarrow r_4 \Rightarrow u_2 = 1, w_{24} = 1$, and the last access $r_4 \Rightarrow u_4 = 1$. For the second sequence $r_1 \rightarrow r_2 \Rightarrow u_1 = 2, w_{12} = 2$, $r_2 \rightarrow r_3 \Rightarrow u_2 = 2, w_{23} = 1$, $r_3 \rightarrow r_4 \Rightarrow u_3 = 1, w_{34} = 1$, and the last access $r_4 \Rightarrow u_4 = 2$. Note that we do not draw edges with 0 weights. The weight of node i can be used to measure the likelihood of the appearance of an access with attribute r_i and the weight of edge e_{ij} can be used to measure the likelihood of the appearance of a transition $r_i \rightarrow r_j$. We use integer values instead of estimations of probabilities because there is insufficient data to characterize the transition probabilities to a certain precision.

3.2. Deviation Scores

The method in Section 3.1 provides a basic data structure to summarize the flow of patients with respect to EMR access information. In this section we introduce several approaches and measures to generate scores that summarize the degree to which the accesses associated with a specific patient appear to deviate. Here, we use L to denote all records in an access log.

Definition 3.1 (*Local Vertex Score*). Given an access log $L : (p, r)$ with attribute $r = r_i \in \mathscr{R}$, and a threshold values $\bar{u} \in \mathbb{R}_+$, the *Local Vertex Score (LVS)* score of L is defined as:

$$LVS(r_i, \bar{u}) = 1_{\{u_i < \bar{u}\}}(\bar{u} - u_i),$$

where A is an event and 1_A is the indicator function defined as:

$$1_A = \begin{cases} 1 & \text{if } A \text{ is true,} \\ 0 & \text{otherwise.} \end{cases} \tag{1}$$

Note that the indicator function implies that the LVS score is the difference $\bar{u} - u_i$ if this is positive and zero otherwise.

Definition 3.2 (*Local Path Score*). Given an access log $L : (p, r)$ with attribute $r = r_i \in \mathscr{R}$, and two threshold values $\bar{u}, \bar{w} \in \mathbb{R}_+$, if it is known that L is in a sequence of access logs $L_1, L_2, \ldots, L_N$ of a particular patient with attribute $r_{i_1}, r_{i_2}, \ldots, r_{i_N}$, which is ordered in the timestamps, then the *Local Path Score (LPS)* of L is defined as:

(1) If $L = L_1$, $LPS(r_i, \bar{u}, \bar{w}) = LVS(r_i, \bar{u}) + \frac{1}{2} 1_{\{w_{i_1 i_2} < \bar{w}\}}(\bar{w} - w_{i_1 i_2})$;
(2) If $L = L_t$ and $t \in \{2, \ldots, N-1\}$, $LPS(r_i, \bar{u}, \bar{w}) = LVS(r_i, \bar{u}) + \frac{1}{2}(1_{\{w_{i_{t-1} i_t} < \bar{w}\}} \times (\bar{w} - w_{i_{t-1} i_t}) + 1_{\{w_{i_t i_{t+1}} < \bar{w}\}} \times (\bar{w} - w_{i_t i_{t+1}}))$;
(3) If $L = L_N$, $LPS(r_i, \bar{u}, \bar{w}) = LVS(r_i, \bar{u}) + \frac{1}{2} 1_{w_{i_{N-1} i_N} < \bar{w}} \times (\bar{w} - w_{i_{N-1} i_N})$.

Definition 3.3 (*Global Path Score*). Given a sequence of access logs $P_L : L_1, \ldots, L_N$ with attribute $P_R : r_{i_1}, r_{i_2}, , r_{i_N}$ of a patient and two threshold values $\bar{u}, \bar{w} \in \mathbb{R}_+$, the *Global Path Score (GPS)* of P_L is defined as:

$$GPS(P_R, \bar{u}, \bar{w}) = \sum_{t=1}^{N} LPS(r_{i_t}, \bar{u}, \bar{w}).$$

Definition 3.4 (*Average Global Path Score*). The *Average Global Path Score (AGPS)* of P_L is defined as:

$$AGPS(P_R, \bar{u}, \bar{w}) = \frac{1}{N} GPS(P_R, \bar{u}, \bar{w}).$$

Let us take a moment to provide some insight into these definitions. First, the function $1_{\{u_i < \bar{u}\}}(\bar{u} - u_i)$ measures the difference between u_i and the desired likelihood $\bar{u}$. A similar interpretation applies to the function $1_{\{w_{ij} < \bar{w}\}}(\bar{w} - w_{ij})$. Additionally, the $\frac{1}{2}$ used to define the LVS score reflects the fact that both vertices of a link contribute to the deviation measure. Thus, the LPS score corresponds to the sum of all the deviations; the difference between the likelihood u_i, w_{ij} and the thresholds $\bar{u}$, $\bar{w}$. As a result, the local scores (LVS and LPS) measure the strength of irregularity of a particular access. By contrast, the global scores (GPS and AGPS) measure the irregularity of a given access path. In combination, these measures summarize the relative irregularity of the accesses for a patient. For example, consider the example graph depicted in Figure 1. Now, imagine a new sequence $P_R : r_1 \to r_3 \to r_4$ with thresholds $\bar{u} = 2$ and $\bar{v} = 1$. Then the LVS scores for these three accesses can be calculated as: $LVS(r_1, \bar{u}) = 0$, $LVS(r_3, \bar{u}) = 2 - 1 = 1$, $LVS(r_4, \bar{u}) = 0$. The LPS scores are: $LPS(r_1, \bar{u}, \bar{v}) = 0 + \frac{1}{2} \times 1 = 0.5$, $LPS(r_3, \bar{u}, \bar{v}) = 1 + \frac{1}{2} \times 1 = 1.5$, $LPS(r_4, \bar{u}, \bar{v}) = 0$. The GPS score for P_R is: $GPS(P_R, \bar{u}, \bar{v}) = 0.5 + 1.5 + 0 = 2$ and the AGPS for P_R is: $AGPS(P_R, \bar{u}, \bar{v}) = \frac{2}{3}$.

3.3. A Heuristic for Threshold Values based on Graph Stability

The scoring functions in Section 3.2 require the specification of two threshold values: $\bar{u}$ and $\bar{w}$, which characterize the likelihood of the occurrence of each node and edge, respectively. When an observed value for a node or edge in a flow is smaller than the threshold, it contributes to the deviation score.

The thresholds can be set by system administrators based on experience, but could also be automatically inferred from historical data. Here, we introduce a data-driven heuristic to determine these two values. This heuristic is based on the assumption that patient record access patterns do not significantly change over time. For example, the pattern in the previous month of data should be similar to the pattern in the next month's dataset. This does not imply that the system is static, but that the statistical model that summarizes flows in the system is relatively constant.

Let us assume that the size of the historical dataset is of size nm, which we partition into n subsets, referred to as Subset 1 through Subset n. Since our basic training unit is an access sequence for one patient, each dataset contains an equal number of access sequences. Next, let $G^k = (V^k, E^k)$ with weights u_i^k and w_{ij}^k be the graph model constructed by applying Algorithm 1 on Subset k. Given thresholds $\bar{u}$ and $\bar{w}$, let the sets of nodes and edges with weights exceeding the threshold values $\bar{u}$ and $\bar{w}$ be:

$$\bar{V}^k(\bar{u}) := \{v_i \in V^k | u_i \geq \bar{u}\},\ \bar{E}^k(\bar{w}) := \{e_{ij} \in V^k | w_{ij} \geq \bar{w}\}. \tag{2}$$

Based on these sets, we invoke $\bar{V}^k(\bar{u})$ and $\bar{E}^k(\bar{w})$ to compare the nodes and edges with weights that do not contribute to the deviation scores (because we anticipate these will be stable patterns). For $k = 1, \ldots, n-1$, the stability of the nodes for the comparison subset k versus subset $k+1$ is measured by a node similarity ratio, defined as:

$$NSim(k, k+1) = \min\left\{\frac{|\bar{V}^k(\bar{u}) \cap \bar{V}^{k+1}(\bar{u})|}{|\bar{V}^k(\bar{u})|}, \frac{|\bar{V}^k(\bar{u}) \cap \bar{V}^{k+1}(\bar{u})|}{|\bar{V}^{k+1}(\bar{u})|}\right\}, \tag{3}$$

$$\overline{NSim} = \frac{1}{n-1}\sum_{k=1}^{n-1} NSim(k, k+1), \tag{4}$$

where $|A|$ is the number of elements in a set A. Similarly, the stability of the edges for the comparison Subset k vs. Subset $k+1$ is measured by an edge similarity ratio, defined as:

$$ESim(k, k+1) = \min\{\frac{|\bar{E}^k(\bar{w}) \cap \bar{E}^{k+1}(\bar{w})|}{|\bar{E}^k(\bar{w})|}, \frac{|\bar{E}^k(\bar{w}) \cap \bar{E}^{k+1}(\bar{w})|}{|\bar{E}^{k+1}(\bar{w})|}\}, \tag{5}$$

$$\overline{ESim} = \frac{1}{n-1}\sum_{k=1}^{n-1} ESim(k, k+1). \tag{6}$$

Note that $\bar{V}^k(1)$ and $\bar{E}^k(1)$ contain all of the nodes and edges appearing in the training dataset, respectively.

We define the node coverage ratio NCR and edge coverage ratio ECR for Subset k as:

$$NCR^k(\bar{u}) = \frac{|\bar{V}^k(\bar{u})|}{|\bar{V}^k(1)|},\ ECR^k(\bar{w}) = \frac{|\bar{E}^k(\bar{w})|}{|\bar{E}^k(1)|} \tag{7}$$

to measure the fraction of nodes and edges used to calculate the deviation scores. The choice of the threshold values $\bar{u}$ and $\bar{w}$ are determined by a balance of the coverage

Table I. A Summary of the Attributes of the Northwestern EMR Access Logs

Attribute	**Description**
User ID	Login credentials (de-identified)
Patient ID	Medical record number (de-identified for cohort)
User Position	Assigned role within the system
Date and Time Stamp	Randomly shifted date for de-identification purposes
Chart Access Reason	Option selected when a chart is first accessed by each user during a hospitalization. Options available are tied to the User Position
Orders Entered	Indicates the number of orders entered by the user during the current chart access (not used in this study)
Location	Location of the patient within the hospital
Service	Hospital service caring for the patient as specified by the doctors caring for the patient

Table II. Summary Statistics of the NMH Dataset Utilized in this Study

	User ID	**Patient ID**	**User Position**	**Chart Access Reason**	**Locations**	**Services**	**Accesses**
Total	8099	16561	131	143	48	37	1,145,852

Table III. Summary Statistics of the Patient Access Paths

# of Paths	**Minimum Length**	**Maximum Length**	**Average Length**	**# of Paths with Loops**
16,561	1	849	68.58	16,539

ratio and the similarity ratio. A high coverage ratio may imply overfitting, whereas a low similarity ratio may result in a model with too much noise. We use α and β to represent the desired levels of coverage and similarity ratio, respectively. Given these levels, we select the minimum values of $\bar{u}$ and $\bar{w}$, such that $NCR^k(\bar{u}), ECR^k(\bar{w}) \leq \alpha$ and $\overline{NSim}, \overline{ESim} \geq \beta$.

4. AN EMPIRICAL STUDY

4.1. Dataset

The dataset for this study was obtained from Northwestern Memorial Hospital (NMH), which is the primary teaching hospital for the Feinberg School of Medicine at Northwestern University. All clinicians, including physicians and nurses, retrieve clinical content and enter inpatient notes and orders online using the Cerner Corporation's PowerChart EMR system. For this analysis, we were provided with the access logs for a three-month period in the year 2010. The attributes of the access logs and the basic summary statistics for the accesses are reported in Tables I and II, respectively. There were a total of 1,145,852 accesses for 16,561 patients in the dataset, which is an average of 69 accesses per patient. For the purposes of this study, the access logs were grouped according to the patient's ID and sorted by the timestamp. Therefore, the accesses of each patient can be considered as a *path*. We provide some statistics of the access paths in Table III. While there were no specific accesses identified as cases of misuse or abuse a priori, we use this dataset to model routine behaviors, upon which we can inject and detect anomalous instances. As such, the results reported here are an approximation of the performance of the system (certain events may be false negatives).

We utilize this data to conduct our analysis as follows. Based on discussions with hospital administrators, it was anticipated that sequence patterns in the access logs would be contingent on the medical service type of the patient. To account for this

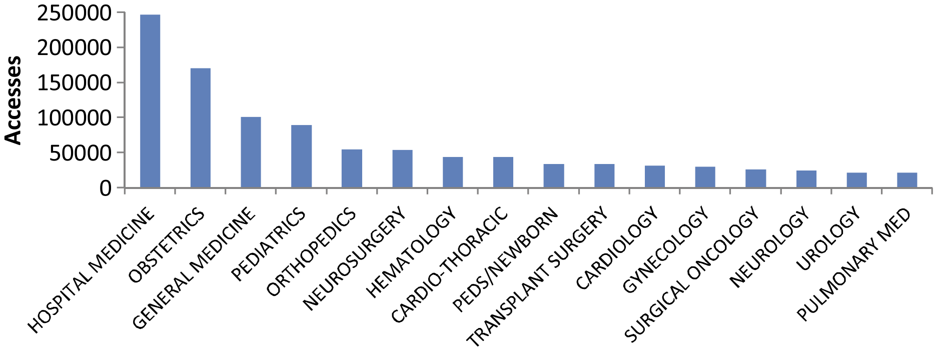


Fig. 2. Number of accesses per service type.

Table IV. The Summary of Hospital Medicine Service with Thresholds $\bar{u} = 1$ and $\bar{w} = 1$

	Subset 1	Subset 2	Subset 3	Subset 4
# of edges	4516	4293	4358	4303
Edge density	22.08%	20.99%	21.31%	21.04%
# of nodes	123	119	120	121
Node density	86.01%	83.21%	83.91%	84.61%
Subset k vs $k+1$	1 vs 2	2 vs 3	3 vs 4	$\overline{NSim}$
# of edges only in subset k	1205	1031	1094	74.3%
# of edges only in subset $k+1$	982	1096	1042	$\overline{ESim}$
# of common edges	3311	3262	3261	95.1%
# of nodes only in subset k	9	4	4	
# of nodes only in subset $k+1$	5	5	5	
# of common nodes	114	115	116	

expectation, we partitioned the data according to the Service attribute. As noted in Table II, this split yields 37 subgroups. Figure 2 summarizes the number of access transactions for categories with at least 20,000 accesses. For this study, we focused on the four largest categories: General Medicine, Hospital Medicine, Obstetrics, and Pediatrics. For each subgroup, a graph model (as described in the following) was constructed with the Chart Access Reason attribute, where the weights were trained using 25% of the data. There are a total of 143 different values for the attribute Chart Access Reason. This attribute was chosen in the analysis because there are no missing values for this attribute. The remaining 75% of the data was used to identify outliers with respect to the constructed graph model and the access evaluation scores. This experimental setup was adopted because the graph is expected to evolve temporally, and a multifold cross validation technique was deemed to be appropriate for such a setting.

4.2. Choice of the Threshold Values $\bar{u}$ and $\bar{w}$

We implemented the heuristic in Section 3.3 on the dataset described in Section 4.1 to specify $\bar{u}$ and $\bar{w}$ as follows. We divided the dataset into four equally-sized temporal subsets (referred to as Subset 1 through Subset 4) and constructed the PFAD model as described in Section 3. We then compared graph stability properties in adjacent subsets. For example, we compared the graphs from Subsets 1 and 2, then Subsets 2 and 3, and finally Subsets 3 and 4. Table IV summarizes the graph stability properties of the Hospital Medicine service with thresholds $\bar{u} = \bar{w} = 1$.

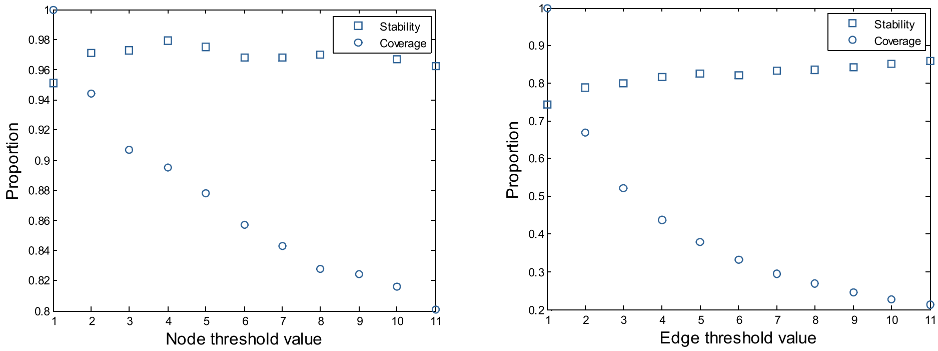


Fig. 3. The stability and coverage ratios for the graph model for the Hospital Medicine service: (left: nodes, right: edges).

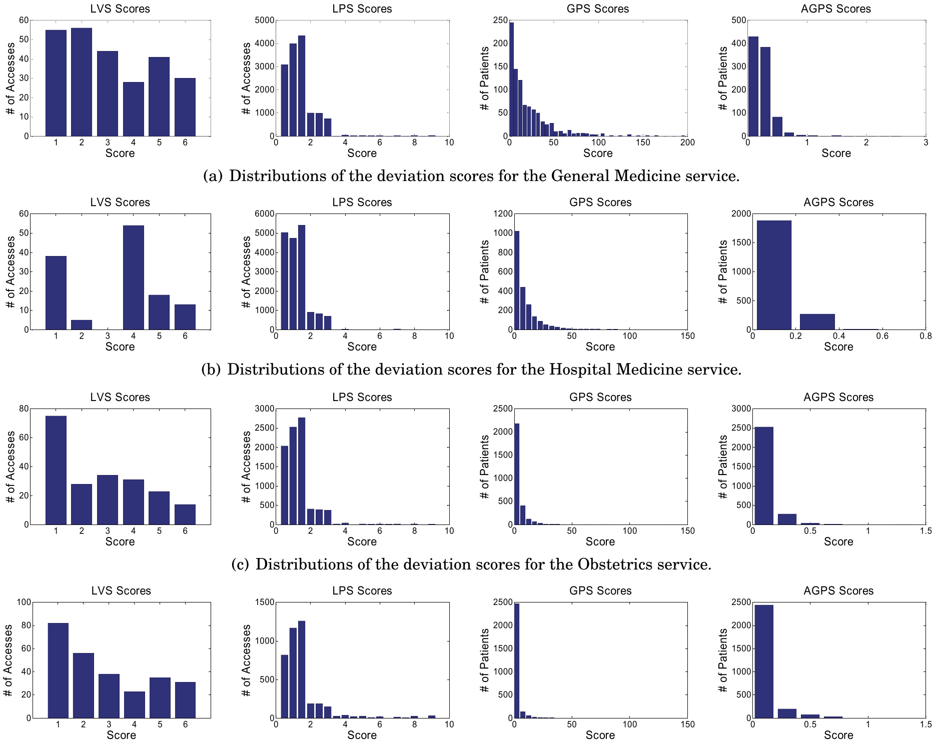
In Table IV, the entries for edges and nodes correspond to the number of such objects with weights u_i and w_{ij} no less than the threshold values. We calculated the coverage ratios $NCR^k(\bar{u})$ and $ECR^k(\bar{w})$ for each subset for different values of $\bar{u}$ and $\bar{w}$.

We computed the quantities listed in the first column of Table IV for each value of $\bar{u} = 1, 2, \ldots, 11$ and $\bar{w} = 1, 2, \ldots, 11$. The relationship between stability and coverage ratios is shown in Figure 3. We also calculated the stability and coverage of the other 3 services (Hospital Medicine, Obstetrics, and Pediatrics). The results for these services were similar and are not reported in this manuscript due to space constraints. To choose appropriate values for the thresholds, we consider two criteria to mitigate overfitting: (1) the coverage ratio should be no greater than 85% and (2) the stability parameter should be no less than 80%. The selection of these two numbers is a trade-off between stability and coverage. The first criterion is designed to prevent fitting our model to noise in the dataset, whereas the second is designed to prevent overfitting to overly specific flow patterns. We choose the smallest values of $\bar{u}$ and $\bar{w}$ for which the coverage ratio is no greater than 85% and the stability parameter is no less than 80%. Based on these criteria, the threshold values for the case study discussed in the following section were set to $\bar{u} = 6$ and $\bar{w} = 3$.

4.3. Properties of the Deviation Scores

For each of the four services types, we constructed the PFAD graph based on 25% of the dataset and calculated the deviation scores for the remaining 75%. Figures 4(a) through 4(d) provide a summary of the score distributions in these four services.

The results in Figures 4(a)–4(d) show that, for each service, only a small portion of accesses lead to high scores. This suggests that an administrator could choose a threshold (for scores) to determine accesses that warrant further investigation. For example, for the General Medicine service, if the threshold of LVS score is chosen to be 4, there are 41 and 30 instances with a score of 5 and 6, respectively. There would therefore be 71 access transactions promoted for further investigation. Similar actions can be applied to LPS, GPS, and AGPS. Note here that in contrast to LVS and LPS, the GPS and AGPS are for complete patient flows, as opposed to specific accesses. For each patient, the GPS and AGPS provide an overall evaluation for his access. Additionally, the four scores provide a characterization of the differences between the patterns of the new and historical access logs. At the same time, it can be seen that the distributions of the four scores do not exhibit a systematic pattern, which implies that the deviation patterns differ across services. We recognize that a single run of the



(a) Distributions of the deviation scores for the General Medicine service.

(b) Distributions of the deviation scores for the Hospital Medicine service.

(c) Distributions of the deviation scores for the Obstetrics service.

(d) Distributions of the deviation scores for the Pediatrics service.

Fig. 4. Distributions of the deviation scores.

system is insufficient to make claims of statistical significance, but believe the results are sufficient to demonstrate a proof-of-concept.

4.4. Analysis of Identified Deviations

We now use the LPS to analyze the deviations associated with nodes (access reasons) and edges (reason transitions). We use LPS in this and subsequent analyses because they are the most primitive combination of access-reason and access-reason-transition deviation. Both GPS and AGPS are constructed from LPS.[1] We analyze the node and edge deviations separately. Note that node (and edge) deviation corresponds to the difference between the node (and edge) weight and the threshold $\bar{u}$ ($\bar{w}$). We count the frequency of nodes with weights less than the threshold value $\bar{u}$ (accesses with positive deviation scores). The results from Figure 5 suggest that most accesses with high node deviation scores are not from physicians. Certain access reasons, such as *AP-Transcriptionist*, *Anesthesia Tech*, *Assigned Tech*, and *Social Worker, Psych* for the General Medicine service) produce more accesses with high node deviation scores. This suggests that these reasons do not follow a regular pattern when accessing patient EMRs. By contrast, there are other access reasons, such as *Customer Service Coordinator*, *Help Desk 1 troubleshooting*, which follow a more consistent pattern.

The results for the edges contributing to positive LPS values are shown in Figure 6. Our methodology counts the frequency of transitions with weights less than the threshold value $\bar{w}$ (transition with positive deviation scores) in the 75% testing

[1] LVS values do not have access reason transition information.

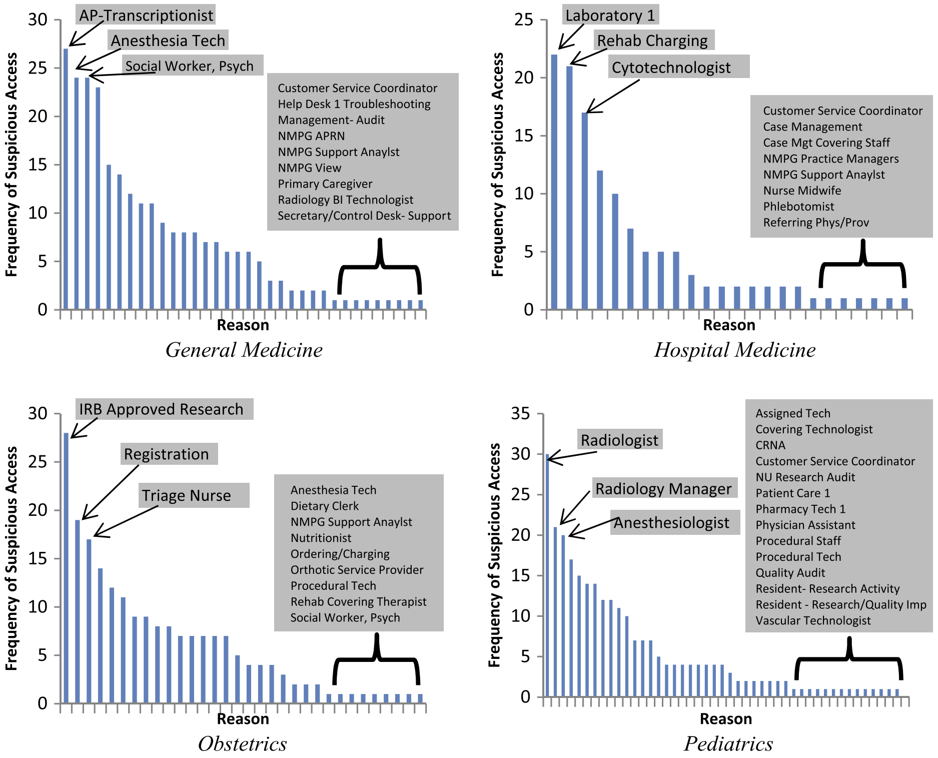


Fig. 5. Frequency of reasons with positive contribution to the LPS scores.

dataset. For simplicity, we only pick the top 10 transitions for each service. The results suggest that a small proportion of transitions contribute significantly to the LPS scores. The transitions between users who do not relate to clinical procedures will be more irregular. Also, transitions between nurses and users who do not have clinical responsibilities behave inconsistently as well.

The reasons for access in this dataset are strongly correlated with the user role. Each user often has only one access reason in the system, therefore, we do not analyze the distribution of the access reasons per role.

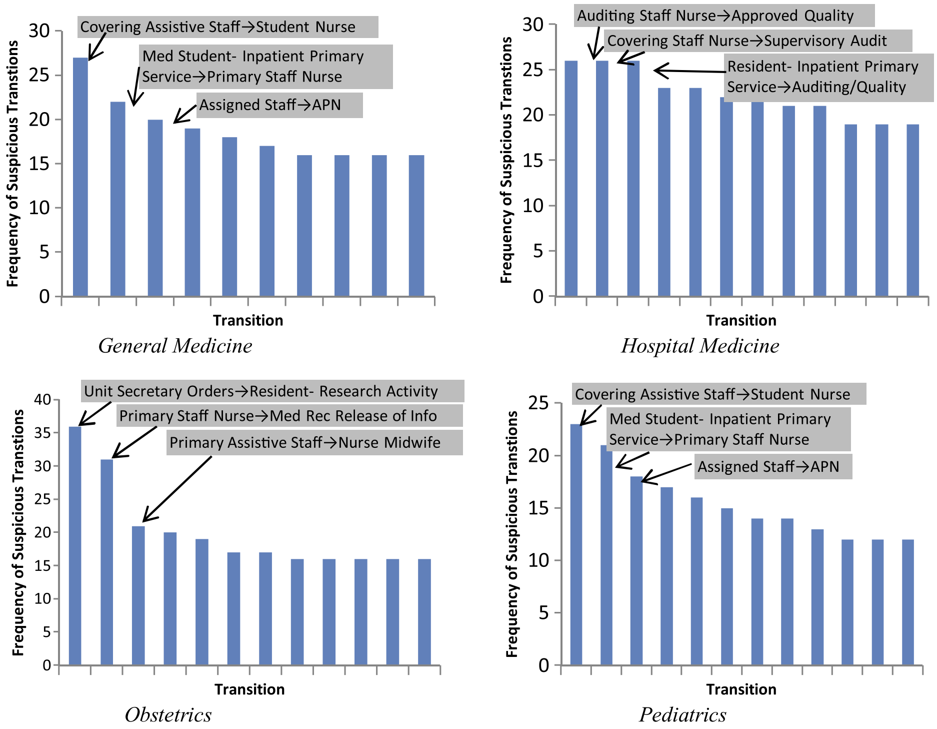
5. SIMULATION RESULTS FOR EFFECTIVENESS OF PFAD

In this section, we use two simulated environments to assess the intrusion detection effectiveness of PFAD. We then compare PFAD with a specialized network anomaly detection model (SNAD) [Chen et al. 2012b]. In lieu of knowledge of actual incidents, the random simulation enables a controlled evaluation of the anomaly detection strategies.

5.1. Performance of PFAD in Simulated Environments

We use two simulation setups, which are defined as follows:

(1) *Randomized User Simulation (RUS)*. In the first simulation setup, we select a user at random, and randomize the access reason R of all his accesses. The randomization for each access follows the procedure in which we randomly pick a reason and



General Medicine *Hospital Medicine*

Obstetrics *Pediatrics*

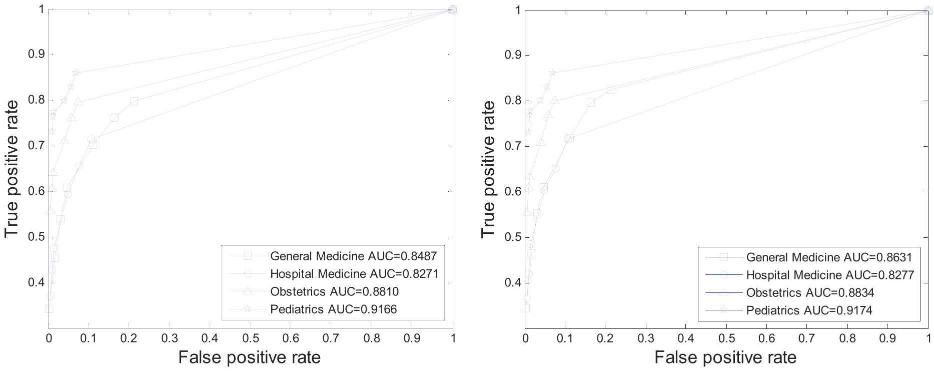
Fig. 6. Frequency of transitions with high contribution to the LPS scores.

substitute the original reason. We then execute the detection model. This process is repeated 100 times.

(2) *Randomized Reason Simulation (RRS).* In this simulation, we randomly select a set of users and randomize one access of each selected user. The access randomization strategy is the same as the first simulation. We perform this analysis over 100 users in one run and perform a total of 100 runs.

To randomize the access reason, we randomly change the order of care in the patient care process. For example, assume that "Primary Staff Nurse → Attending Physician → Billing" is a reason sequence. We randomly pick "Billing", and change it to another reason, "Pharmacist", which was picked at random. These simulations are used to evaluate whether the system can detect this change as a deviated transition.

For each simulation, we use the LPS value and provide the anomaly detection rates of PFAD under different false positive rates. The false positive rate for a given threshold score is calculated as the number of nonrandomized accesses with LPS scores above the threshold divided by the total number of nonrandomized accesses. The true positive rates are calculated by dividing the number of randomly revised accesses with anomaly scores above the threshold by the total number of randomly revised accesses. We choose different threshold scores to calculate both rates. For each false positive rate, we resample 25% data for 30 times. In each resampling, we run 100 simulations to calculate the average detection rate. The results are summarized in Figures 7(a) and 7(b). The area under the ROC curve (AUC) values for all four service types suggest the effectiveness of PFAD. Specifically, it can be seen that in a randomized user scenario, the AUC ranges from 0.83 for Hospital Medicine to 0.92 for Pediatrics. Similar results were found in the randomized reason scenario.



(a) Randomized User

(b) Randomized Reason

Fig. 7. ROC curves for the PFAD model in various simulation settings.

5.2. Comparison with SNAD

In this section we compare PFAD with a variation of the Specialized Network Anomaly Detection algorithm (SNAD) [Chen et al. 2012b] under the two simulation setups presented in Section 5.1. We chose SNAD because it also uses a graph-based model and has been shown to be more effective and efficient compared to other strategies (e.g., spectral anomaly detection [Chen and Malin 2011]) when searching for specific anomalous accesses. In the original version of SNAD, a local access network of users is constructed for each patient. It then calculates the similarity of the users' access patterns in the network. SNAD then evaluates each access by comparing the similarity of an access network to a subnetwork that suppresses one of the network's users. When the similarity between the network and subnetwork are significantly different, SNAD claims the suppressed user's access was an anomaly. For this study, we make a generalization of SNAD, so that the local access network is focused on a reason as opposed to a patient. More specifically, our variation on SNAD treats each access as a pair (u, r), where u is the user associated with the access and r is the attribute value; e.g., Chart Access Reason. For access reason r, SNAD establishes a network for all the users who accessed reason r. Based on these networks, SNAD calculates a score for each pair (s, r). For PFAD, we use the LPS score for comparison. A fundamental difference between PFAD and SNAD is that the former learns a model from the training data set and evaluates any new access with the learned model. SNAD, by contrast, only uses the evidence presented in a single time period.

Since running simulations with SNAD is time consuming (see later discussion), we compared the two techniques only at the 1.5% false positive rate. Recall that we first pick a threshold score such that the false positive rate is about 1.5%. For both detection models, we first implement the model without any randomization. For PFAD, we perform 30 runs for each simulation by randomly sampling 25% data each time and use the results to estimate a 95% confidence interval of the mean positive rate. The average runtime of the two models is the average seconds per scored access. The algorithms were implemented in the R statistical software package [R Development Core Team 2008] and all experiments were run on a Dell 6420 using an Intel Core i5-2520M 2.50GHz with 4GB of RAM using 32-bit Windows 7.

Table V summarizes the results of the comparative analysis. First, it can be seen that SNAD achieves a better detection performance than PFAD for the General Medicine and Hospital Medicine services, whereas PFAD is better for the Obstetrics and Pediatrics services. This implies that these methods may be complementary in practice.

Table V. Summary of Comparison Results between PFAD and SNAD

Service	RUS		RRS		Average runtime	
	PFAD	SNAD	PFAD	SNAD	PFAD	SNAD
General Medicine	(45.13%, 45.67%)	**71.2%**	(45.26%, 45.58%)	**61.4%**	$\mathbf{2.44 \times 10^{-5}}$	0.522
Hospital Medicine	(46.92%, 47.43%)	**70.3%**	(47.64%, 47.99%)	**61.7%**	$\mathbf{2.63 \times 10^{-5}}$	0.297
Obstetrics	(**63.44%**, **63.63%**)	57.5%	(**62.02%**, **63.07%**)	52.0%	$\mathbf{2.63 \times 10^{-5}}$	0.117
Pediatrics	(**77.52%**, **77.85%**)	58.5%	(**77.43%**, **77.71%**)	53.7%	$\mathbf{2.57 \times 10^{-5}}$	0.222

Intuitively, patients in Obstetrics and Pediatrics follow standard procedures so the sequential pattern-based deviations will be less significant. The patient care procedures contain more randomness for patients in General Medicine and Hospital Medicine, both of which admit patients with a larger variety of medical conditions. For these situations, PFAD in its current form, is likely to be less effective.

Second, PFAD has similar performance for both randomized user and reason scenarios, whereas SNAD performs better for the randomized user. This is because all of the accesses of one user were randomized in the randomized user setting, which implies that the behavior of this user has changed significantly. However, in the randomized reason, we only revise one access of each user. Since PFAD focuses on the patterns at the level of an access reason and an access reason transition, its performance is stable for both settings. The different true positive detection rates for the four services suggest that the patterns in different services are different, so partitioning the dataset according to the hospital service type is important.

Finally, it is clear that PFAD can achieve its computation much faster than SNAD, which is important when an HCO needs to process a large amount of data in a short amount of time. Consider, in this dataset, there are more than $50,000$ accesses. The total runtime for processing this data daily is less than $50000 \times 2.63 \times 10^{-5} \approx 1.5$ seconds. The worst-case running time for SNAD for such a dataset is $50000 \times 0.522 \approx 7$ hours. This significant difference is made clearer when we look into the computational complexity of the algorithms. The runtime complexity of SNAD is $O(m \times \log m \times (\log n)^2)$, where m is the number of possible values of attribute R and n is the number users. For PFAD, graph construction takes $O(m)$ effort. Then each new access is compared with the corresponding weight in the graph, which requires $O(1)$ time. Clearly, PFAD will scale to larger medical record access logs at a more graceful rate than SNAD. Moreover, the results suggest a potential to support online computing in large information systems.

6. DISCUSSION AND CONCLUSIONS

In this article, we proposed a graph-based framework for scoring the irregularity of EMR users' accesses in a temporal setting. In the model, vertices represent the total number of a selected attribute R and the edges are used to represent the order information of the accesses for each patient. Based on the graph model, we proposed four types of measures to capture irregularity at the level of a local access and a global path for a patient's EMR. These scores can be used to evaluate individual accesses and the access path of each patient. We demonstrated this methodology using one particular attribute (Chart Access Reasons) in a real dataset of accesses to inpatient medical records at a large hospital. Since most EMR systems can provide a timestamp for each access, our methodology can be readily expanded to different systems for different attributes. For instance, while our investigation focused on the Chart Access Reason, the approach readily generalizes to other attributes, such as hospital location or medical service caring for the patient. Moreover, each attribute could be weighted according to relative importance. The main contribution of this methodology can be summarized as follows: (1) it provides a clear and convenient way to support a system administrator in the analysis of access logs; (2) it has low complexity with good performance; (3) it can be easily extended to any information system with access logs that can be grouped according to each task and represented by sequences. We believe that the patient-flow-based approach provides a new perspective on EMR auditing and may assist hospital privacy officials in their investigative activities.

From an empirical perspective, we showed that this framework can appropriately segment the system into patterns of flows, from which only a small portion of accesses sufficiently deviate to raise an alarm. In the process, we showed that a small number of reasons and transitions between reasons contribute to a majority of deviation scores. We wish to highlight that the deviation pattern varies among different hospital services. As a specific example, we observed that that nonclinical users tend to exhibit greater deviations from such access patterns, suggesting that greater access control for this user group may improve EMR security.

At the same time, there are several limitations of the current work that we wish to point out. First, since our method is data-driven, it requires a nontrivial amount of data to train the graph-based model. This may be problematic when the number of elements for the studied attribute is large. Additionally, it should be recognized that patterns in EMRs may evolve over time [Malin et al. 2011] and exhibit seasonal dependencies. It is thus recommended that the graph-based models, be retrained after a certain amount of time. Further research should investigate the stability of such patterns over long time frames. Second, our model is restricted to a one-step transition model, which limits the sequential pattern that can be represented and leveraged for anomaly detection. Third, the four scores utilized by our model are biased to detect uncommon events, which may, in certain instances, be acceptable. Fourth, our one-step transition analysis illustrates the power in modeling the progression of reasons, but should be extended to consider time between events. Fifth, this study focused on the detection of simulated anomalies in the context of real data, but did not determine if any of the false positives were in fact, suspicious anomalies. It will be useful to review all detected anomalies with privacy officials, who may be able to provide an interpretation of the deviation patterns. Despite these limitations, our strategy identifies novel types of anomalies that can supplement a larger security framework. It can be readily combined with other EMR anomaly detectors (e.g., SNAD) and, when necessary, be preempted by knowledge supplied by HCO experts to ensure that certain exceptions are always granted.

ACKNOWLEDGMENTS

The authors would like to thank Dr. You Chen of Vanderbilt University for providing useful guidance on application of the SNAD algorithm.

REFERENCES

Amatayakul, M. 2009. Think a privacy breach couldn't happen at your facility? *Hospital Financial Manage. 12*, 61–65.

Appari, A. and Johnson, M. 2011. Information security and privacy in healthcare: Current state of research. *Int. J. Internet Enterprise Manage. 6*, 279–314.

Asaro, P. V. and Ries, J. E. 2001. Data mining in medical record access logs. In *Proceedings of the American Medical Informatics Association Annual Symposium*. 855.

Ash, J. S., Berg, M., and Coiera, E. 2004. Some unintended consequences of information technology in health care: The nature of patient care information system-related errors. *J. Amer. Med. Informatics Assoc. 11,* 2, 104–112.

Bansal, G., Zahedi, F., and Gefen, D. 2010. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Syst. 49*, 138–150.

Bhatti, R. and Grandison, T. 2007. Towards improved privacy policy coverage in healthcare using policy refinement. In *Proceedings of the Secure Data Management Workshop 4721*, 158–173.

Blobel, B. 2004. Authorisation and access control for electronic health record systems. *Int. J. Med. Informatics 73,* 3, 251–257.

Bosch, M., Faber, M. J., Cruijsberg, J., Voerman, G. E., Leatherman, S., Grol, R. P., Hulscher, M., and Wensing, M. 2009. Review article: Effectiveness of patient care teams and the role of clinical expertise and coordination: A literature review. *Med. Care Res. and Rev. 66,* 6 Suppl., 5S–35S.

Boxwala, A. A., Kim, J., Grillo, J. M., and Ohno-Machado, L. 2011. Using statistical and machine learning to help institutions detect suspicious access to electronic health records. *J. Amer. Med. Informatics Assoc. 18*, 498–505.

Buntin, M. B., Jain, S. H., and Blumenthal, D. 2010. Health information technology: Laying the infrastructure for national health reform. *Health Affairs 29,* 6, 1214–1219.

Campbell, E. M., Sittig, D. F., Ash, J. S., Guappone, K. P., and Dykstra, R. H. 2006. Types of unintended consequences related to computerized provider order entry. *J. Amer. Med. Informatics Assoc. 13,* 5, 547–556.

Campbell, H., Hotchkiss, R., Bradshaw, N., and Porteous, M. 1998. Integrated care pathways increase use of guidelines. *British Med. J. 316*, 133–137.

Cavusoglu, H., Mishra, B., and Raghunathan, S. 2005. The value of intrusion detection systems in information technology security architecture. *Inform. Syst. Res. 16,* 1, 28–46.

Chaudhry, B., Wang, J., Wu, S., Maglione, M., Mojica, W., Roth, E., Morton, S. C., and Shekelle, P. G. 2006. Systematic review: Impact of health information technology on quality, efficiency, and costs of medical care. *Ann. Intern. Med. 144,* 10, 742–752.

Chen, W.-H., Hsu, S.-H., and Shen, H.-P. 2005. Application of SVM and ANN for intrusion detection. *Comput. Op. Res. 32*, 2617–2634.

Chen, Y. and Malin, B. 2011. Detection of anomalous insiders in collaborative environments via relational analysis of access logs. In *Proceedings of 1st ACM Conference on Data and Application Security and Privacy*. 63–74.

Chen, Y., Nyemba, S., and Malin, B. 2012a. Auditing medical records accesses via healthcare interaction networks. In *Proceedings of the American Medical Informatics Association Annual Symposium*. 93–102.

Chen, Y., Nyemba, S., Zhang, W., and Malin, B. 2012b. Specializing network analysis to detect anomalous insider actions. *Security Informatics 1,* 5, 1–24.

Chou, C., Du, T., and Lai, V. S. 2007. Continuous auditing with a multi-agent system. *Decis. Supp. Syst. 42*, 2274–2292.

Davis, D. and Having, K. 2006. Compliance with HIPAA security standards in U.S. hospitals. *J. Healthcare Inform. Manage. 20*, 108–115.

Dimick, C. 2010. A guide to California's breaches: First year of state reporting requirement reveals common privacy violations. *J. Amer. Health Inform. Manage. Assoc. 81*, 34–36.

Fabbri, D. and LeFevre, K. 2011. Explanation-based auditing. In *Proceedings of the VLDB Endowment*, *5*. 1–12.

Fabbri, D. and LeFevre, K. 2013. Explaining accesses to electronic medical records using diagnosis information. *J. Amer. Med. Informatics Assoc. 20,* 1, 52–60.

Ferreira, A., Correia, R. J. C., Antunes, L., Farinha, P., Oliveira-Palhares, E., Chadwick, D. W., and da Costa Pereira, A. 2006. How to break access control in a controlled manner. In *Proceedings of 19th IEEE International Symposium on Computer-Based Medical Systems*. 847–854.

Gallagher, R. J., Sengupta, S., Hripcsak, G., Barrows, R. C., and Clayton, P. D. 1998. An audit server for monitoring usage of clinical information systems. In *Proceedings of the American Medical Informatics Association Annual Symposium*.

Georgiadis, C., Mavridis, I., Nikolakopoulou, G., and Pangalos, G. 2002. Implementing context and team based access control in healthcare intranets. *Med. Informatics Internet Medicine 27*, 185–201.

Goldberg, I. V. 2000. Electronic medical records and patient privacy. *Health Care Manager 18,* 3, 63–69.

Goldschmidt, P. G. 2005. Hit and mis: Implications of health information technology and medical information systems. *Comm. ACM 48,* 10, 68–74.

Gunter, C. A., Liebovitz, D., and Malin, B. 2011. Experience-based access management: A life-cycle framework for identity and access management systems. *IEEE Security Privacy 9,* 5, 48–55.

Holton, C. 2009. Identifying disgruntled employee systems fraud risk through text mining: A simple solution for a multi-billion dollar problem. *Decision Supp. Syst. 46*, 853–864.

Jakkula, V. R. and Cook, D. J. 2008. Anomaly detection using temporal data mining in a smart home environment. *Methods Inform. Medicine 47,* 1, 70–75.

Jakkula, V. R., Crandall, A. S., and Cook, D. J. 2008. *Advanced Intelligent Environments*. Chapter Enhancing anomaly detection using temporal pattern discovery, 175–194, Spriger.

Kannampallil, T. G., Schauer, G. F., Cohen, T., and Patel, V. L. 2011. Considering complexity in healthcare systems. *J. Biomed. Informatics 44,* 6, 943–947.

Kim, J., Grillo, J. M., Boxwala, A. A., Jiang, X., Mandelbaum, R. B., Patel, B. A., Mikels, D., Vinterbo, S. A., and Ohno-Machado, L. 2011. Anomaly and signature filtering improve classifier performance for detection of suspicious access to ehrs. In *Proceedings of the American Medical Informatics Association Annual Symposium*. 723–731.

King, J. T., Smith, B., and Williams, L. 2012. Modifying without a trace: General audit guidelines are inadequate for open-source electronic health record audit mechanisms. In *Proceedings of the 2nd ACM SIGHIT International Health Informatics Symposium*. 305–314.

Kwon, J. and Johnson, M. 2013. Security practices and regulatory compliance in the healthcare industry. *J. Amer. Med. Informatics Assoc. 20,* 1, 44–50.

Lane, T. and Brodley, C. E. 1999. Temporal sequence learning and data reduction for anomaly detection. *ACM Trans. Inform. Syst. Secur. 2,* 3, 295–331.

Le, X., T. Doll, Barbosu, M., Luque, Z., and Wang, D. 2012. An enhancement of the role-based access control model to facilitate information access management in context of team collaboration and workflow. *J. Biomed. Informatics 45*, 1084–1107.

Lee, H. and Chang, S. 2012. RBAC-matrix-based EMR rights management system to improve HIPAA compliance. *J. Med. Syst 36*, 2981–2992.

Li, X., Xue, Y., and Malin, B. 2012. Detecting anomalous behaviors in workflow-driven web applications. In *Proceedings of the 31st IEEE International Symposium on Reliable Distributed Systems*. 1–10.

Loomis, G. A., Ries, J. S., Saywell, R. M., and Thakker, N. R. 2002. If electronic medical records are so great, why arent family physicians using them? *J. Family Practice 51,* 7, 636–641.

Ludwick, D. A. and Doucette, J. 2009. Adopting electronic medical records in primary care: lessons learned from health information systems implementation experience in seven countries. *Int. J. Med. Informatics 78,* 1, 22–31.

Malin, B., Nyemba, S., and Paulett, J. 2011. Learning relational policies from electronic health record access logs. *J. Biomed. Informatics 44,* 2, 333–342.

Manos, D. September 12 2012. Four reasons for CIOs to celebrate stage 2 meaningful use. *Gov. Health IT Mag.*

Marinovic, S., Craven, R., Ma, J., and Dulay, N. 2011. Rumpole: A flexible break-glass access control model. In *Proceedings of the 16th ACM Symposium on Access Control Models and Technologies*. 73–82.

Menon, A., Jiang, X., Kim, J., Vaidya, J., and Ohno-Machado, L. 2013. Detecting inappropriate access to electronic health records using collaborative filtering. *Mach. Learn.*, 1–1.

Motta, G. and Furuie, S. 2003. A contextual role-based access control authorization model for electronic patient records. *IEEE Trans. Inform. Technol. Biomed. 7*, 202–207.

Park, J. S., Sandhu, R., and Ahn, G.-J. 2001. Role-based access control on the Web. *ACM Trans. Inform. Syst. Secur. 4,* 1, 37–71.

Peleg, M., Beimel, D., Dori, D., and Denekamp, Y. 2008. Situation-Based Access Control: Privacy management via modeling of patient data access scenarios. *J. Biomed. Informatics 41,* 6, 1028–1040.

Pizziferri, L., Kittler, A. F., Volk, L. A., Honour, M. M., Gupta, S., Wang, S., Wang, T., Lippincott, M., Li, Q., and Bates, D. W. 2005. Primary care physician time utilization before and after implementation of an electronic health record: A time-motion study. *J. Biomed. Informatics 38,* 3, 176–188.

Probst, C. W., Hansen, R. R., and Nielson, F. 2007. Where can an insider attack? In *Proceedings of the 4th International Conference on Formal Aspects in Security and Trust*. 127–142.

R Development Core Team. 2008. *R: A Language and Environment for Statistical Computing*. R Foundation for Statistical Computing, Vienna, Austria.

Rostad, L. and Nytro, O. 2006. A study of access control requirements for healthcare systems based on audit trails from access logs. In *Proceedings of the 22nd Annual Computer Security Applications Conference*. 175–186.

Sandhu, R. and Samarati, P. 1994. Access control: Principle and practice. *IEEE Comm. Mag. 32*, 40–48.

Sandhu, R., Coyne, E., Feinstein, H., and Youman, C. 1996. Role-based access control. *IEEE Comput. 26*, 38–47.

Schoenberg, R. and Safran, C. 2000. Internet based repository of medical records that retains patient confidentiality. *British Med. J. 321*, 1199–1203.

Schultz, E. 2002. A framework for understanding and predicting insider attacks. *Comput. Security 21*, 526–531.

Smith, E. and Eloff, J. 1999. Security in health-care information systems—Current trends. *Int. J. Med. Informatics 54*, 39–54.

Stolfo, S., Bellovin, S., Hershkop, S., Keromytis, A., Sinclair, S., and Smith, S. 2008. *Insider Attack and Cyber Security: Beyond the Hacker*. Springer, New York, NY.

Sun, J., Tao, D., and Faloutsos, C. 2006. Beyond streams and graphs: Dynamic tensor analysis. In *Proceedings of KDD*. 374–383.

Ye, N., Li, X., Chen, Q., Emran, S. M., and Xu, M. 2001. Probabilistic techniques for intrusion detection based on computer audit data. *IEEE Trans. Syst., Man, and Cybern. A, Syst. Humans 31,* 4, 266–274.

Zhang, L., Ahn, G.-J., and Chu, B.-T. 2003. A rule-based framework for role-based delegation and revocation. *ACM Trans. Inform. Syst. Security 6,* 3, 404–441.

Zhang, W., Gunter, C. A., Liebovitz, D., Tian, J., and Malin, B. 2011. Role prediction using electronic medical record system audits. In *Proceedings of the American Medical Informatics Association Annual Symposium*. 858–867.

Zhou, Z. and Liu, B. J. 2005. HIPAA compliant auditing system for medical images. *Comput. Med. Imaging Graphics 29,* 2–3, 235–241.

Received December 2012; revised July 2013, October 2013; accepted November 2013