

Explaining accesses to electronic medical records using diagnosis information

Daniel Fabbri, Kristen LeFevre

Electrical Engineering & Computer Science, University of Michigan, Ann Arbor, Michigan, USA

Correspondence to
Daniel Fabbri, Electrical Engineering & Computer Science, University of Michigan, 2260 Hayward Avenue, Ann Arbor, MI 48109, USA;
dfabbri@umich.edu

Received 12 April 2012
Accepted 30 September 2012
Published Online First
2 November 2012

ABSTRACT

Objective Ensuring the security and appropriate use of patient health information contained within electronic medical records systems is challenging. Observing these difficulties, we present an addition to the explanation-based auditing system (EBAS) that attempts to determine the clinical or operational reason why accesses occur to medical records based on patient diagnosis information. Accesses that can be explained with a reason are filtered so that the compliance officer has fewer suspicious accesses to review manually.

Methods Our hypothesis is that specific hospital employees are responsible for treating a given diagnosis. For example, Dr Carl accessed Alice's medical record because Hem/Onc employees are responsible for chemotherapy patients. We present metrics to determine which employees are responsible for a diagnosis and quantify their confidence. The auditing system attempts to use this responsibility information to determine the reason why an access occurred. We evaluate the auditing system's classification quality using data from the University of Michigan Health System.

Results The EBAS correctly determines which departments are responsible for a given diagnosis. Adding this responsibility information to the EBAS increases the number of first accesses explained by a factor of two over previous work and explains over 94% of all accesses with high precision.

Conclusions The EBAS serves as a complementary security tool for personal health information. It filters a majority of accesses such that it is more feasible for a compliance officer to review the remaining suspicious accesses manually.

INTRODUCTION

The security and appropriate use of the personal health information (PHI) contained within medical records is becoming increasingly important as medical records transition from paper to digital form. In the USA, legislation such as the Health Insurance Portability and Accountability Act and the Health Information Technology for Economic and Clinical Health Act outline rules governing the appropriate use of PHI by hospital employees. To monitor and ensure that these rules are followed, modern electronic medical records (EMR) systems maintain an audit log that records all accesses to PHI, which compliance officers can retrospectively review. Ideally, such a system would deter inappropriate behavior.

Unfortunately, even with these auditing systems in place, there have been numerous well-publicized instances of hospital employees inappropriately accessing PHI. For example, various celebrities and dignitaries from Britney Spears to Congresswoman

Gabrielle Giffords have had their PHI breached.^{1 2} In many cases, employees are not malicious, but rather are simply curious. As stated by a healthcare employee, "It's pretty damn common' for medical professionals to peek at files for unwarranted reasons".³ While some curious accesses result in punishment or termination, many go unnoticed.

Ensuring the appropriate use of PHI is difficult due to the complexities of the medical work environment. First, patient care is dynamic, personalized and often involves many hospital employees. As a result, it is difficult to determine who will treat a patient and require access to his medical record. Second, because it is not known who will treat a patient (especially in emergency situations), EMR typically do not deploy fine-grained access controls to limit access to specific medical records.⁴ Therefore, once a hospital employee is authenticated by the EMR system, the employee can access any patient's medical record, which makes PHI susceptible to curious behavior. Third, the number of accesses to EMR is very large (the University of Michigan Health System generates over 4 million accesses per week), and employees are generally well behaved, meaning that finding the few inappropriate accesses is like finding a needle in a haystack. While it is the compliance officer's responsibility to monitor the audit log, there are limits to how many accesses can practically be analyzed in a given time. In practice, compliance officers monitor accesses to VIPs or patients who have registered a complaint, but no additional monitoring is provided to the general public.

Observing these challenges, and the limitations of the current auditing infrastructure, we present an explanation-based auditing system (EBAS) to enhance medical record security. Our insight is that most appropriate accesses to medical records occur for valid clinical or operational reasons in the process of treating a patient, while inappropriate accesses do not. This insight is exemplified with the University of Michigan Health System's screen saver: 'Authorized access is limited to those with the need to know for purposes of patient care, billing, medical record review, or quality assurance.' As shown in figure 1, the EBAS attempts to determine automatically the clinical or operational reason for a given access in the audit log. If a valid reason is found, the access is classified as appropriate. The compliance officer manually analyzes the remaining suspicious accesses as before. Intuitively, the EBAS serves as a filter on the audit log so that the task of manually reviewing suspicious accesses becomes more feasible.

The challenge for the EBAS is to detect valid reasons for access that are also easily explained.

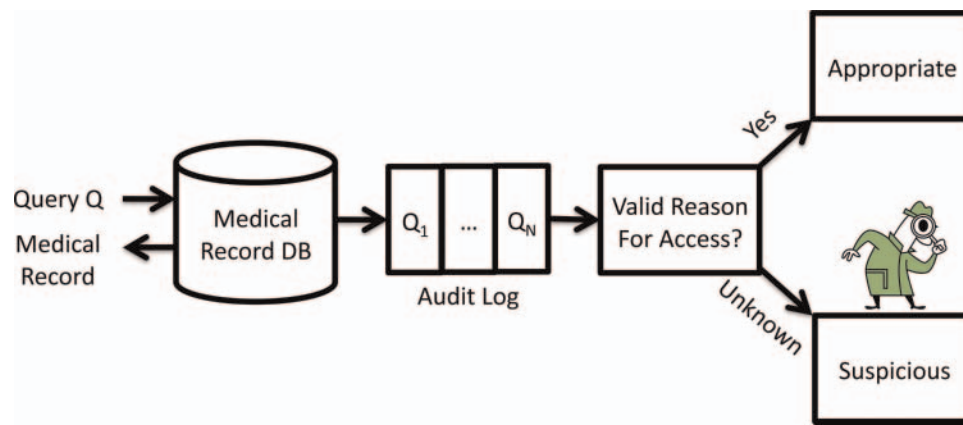


Figure 1 The explanation-based auditing system attempts to find a valid clinical or operational reason for each access in the audit log. Accesses without a reason are suspicious and manually reviewed by the compliance officer. This figure is only reproduced in colour in the online version.

There are several classes of reasons that logically explain why accesses occur. One class relies on the fact that EMR databases store information describing the process by which a patient is treated. For example, the EMR database stores appointment information, medication orders and radiological findings, all of which can be used as evidence to infer the reason for an access based on who participated in the appointment, administered the medication or reviewed the x-ray.^{5 6} Another similar class relies on relationships between patients and hospital employees to infer the reason for an access.^{7 8} For example, the relationship between a patient and his primary physician, or even a physician who works in the same department, serves as a valid reason for access.

The EBAS makes two simplifying assumptions. First, it addresses the threat posed by a curious employee who only accesses PHI; it does not address the potential threat posed by a malicious employee who modifies database information or the threat posed by a malicious outsider who compromises the authentication system. (In this way, the EBAS is complementary to traditional security tools and techniques.) Second, it assumes that all appropriate accesses occur for a valid clinical or operational reason to treat a patient. However, some appropriate accesses occur for alternative reasons such as retrospective research. As a result, the EBAS can produce false positives and negatives. We believe these assumptions strike a reasonable balance between addressing a real and meaningful threat to PHI and addressing the practical aspects of the problem.

To improve the EBAS, this work investigates a new class of explanations for accesses that has not been studied before: diagnosis information. In particular, EMR databases store codes from the International Statistical Classification of Diseases and Related Health Problems, revision 9 (ICD-9) that describe over 6000 diagnoses, diseases and procedures (eg, acne, breast cancer, encounter of chemotherapy), which are later used for billing purposes (for conciseness, this paper uses the term diagnosis to refer to the ICD-9 diagnoses, diseases and procedures). Our hypothesis is that specific hospital employees are responsible for treating each diagnosis (ie, ICD-9 code) and that a group of employees treat a diagnosis together. The challenge is to determine which employees are responsible for each diagnosis.

The results and discussion section shows that integrating diagnosis responsibility information into the auditing system increases the number of appropriate accesses that can be explained. Previous work explained accesses by finding connections between the patient whose record was accessed and the

employee accessing the patient's record.^{5 6} However, EMR databases are often missing information to make these connections. In the case of diagnosis information, while the database stores each patient's diagnoses, it does not store which employees are responsible for treating each diagnosis. By adding fine-grained information describing which employees are responsible for treating each diagnosis, additional connections can be discovered and more appropriate accesses can be explained.

OBJECTIVE

The goal of the EBAS is to determine if a given access occurred for a valid clinical or operational reason to treat a patient. Previous work (eg, Chen and Malin)⁹ focused on finding individual employees who consistently displayed anomalous behavior across many accesses (eg, downloading large amounts of patient data). However, in the medical domain, there is another threat: individual employees who are generally well behaved, but who have occasional instances of curiosity that lead to inappropriate accesses. Our work thus focuses on discovering individual inappropriate accesses, rather than finding users who consistently display anomalous behavior.

We first describe what information is available to the auditing system to determine if an access is appropriate. An access is stored in the audit log as an audit log entry that describes the employee who accessed the EMR system, the patient whose record was accessed, and the time of the access (ie, Audit Log (employee, patient, timestamp)). The EMR database additionally stores patient information that can be used as evidence to infer the reason for an access, such as appointment and medication information. A reason for access is conceptually represented as a logical expression using information from an audit log entry and the evidence. If satisfied, then the access is explained by the reason and is deemed to be appropriate. For example, an employee accessing a patient's record because of an appointment can be represented as a logical condition on the audit log entry and appointment evidence.⁵

The auditing system works as follows: the auditing system is given as input an audit log entry, the evidence and a set of valid reasons that are approved by the compliance officer. The system outputs whether the access is appropriate or suspicious. If the access is appropriate, the system also outputs the set of reasons that explain why it is appropriate.

Ideally, the auditing system would correctly classify each access such that the suspicious set of accesses contains all inappropriate accesses and no appropriate accesses. However, in

Research and applications

this environment, it is difficult to determine the gold standard label for an access (ie, is the access really appropriate or inappropriate) because of the volume of accesses (4.5 million per week), the compliance officer's limited time to label data manually and restrictions on the data that researchers can view (we were only provided with de-identified data and therefore could not manually label the data ourselves). Instead, for the purpose of evaluating our techniques, we construct a fake audit log as a proxy for inappropriate ('curious') behavior. The fake log is constructed by copying the real audit log, and for each audit log entry, replacing the employee with a randomly selected employee from the hospital system. The resulting fake audit log is of equal size and has the same distribution of diagnoses as the real audit log. This randomness is intended to mimic curious access patterns. Previous work has used similar approaches of inserting random accesses to detect inappropriate behavior.⁹ We acknowledge that the lack of manually labeled data is a limitation of this work, but believe the methodology allows for the effective study of a difficult problem.

Due to the lack of labeled data, the quality of the auditing system's classification is measured by analyzing which real and fake accesses can be explained (ie, labeled as appropriate) as a proxy for correctly labeling appropriate and inappropriate accesses. While this methodology requires the assumption that all accesses in the real log are appropriate and all accesses in the fake log are inappropriate (even though there may be a few inappropriate accesses in the real log or visa versa), it is a reasonable strategy given that employees are generally well behaved.

More formally, this objective can be expressed in terms of recall, precision and F-measure metrics. The recall for a set of reasons R , evidence E and audit log L is the fraction of real accesses explained from the entire real log (a recall of 1.0 implies that all real accesses are explained).

$$\text{Recall}(L, E, R) = \frac{|\text{access} \in L \text{ explained by reasons } R \text{ using evidence } E|}{|L|}$$

The precision for a set of reasons R , evidence E , audit log L and fake audit log F is the fraction of real accesses explained versus real and fake accesses explained (a precision of 1.0 implies that no fake access is spuriously explained).

$$\text{Precision}(L, E, R) = \frac{|\text{access} \in L \text{ explained by reasons } R \text{ using evidence } E|}{|\text{access} \in L \cup F \text{ explained by reasons } R \text{ using evidence } E|}$$

F-measure takes into account the system's ability to classify accesses correctly versus its ability to find all appropriate accesses.

$$\text{F-Measure}(L, F, E, R) = 2 \times \frac{\text{Precision}(L, F, E, R) \times \text{Recall}(L, E, R)}{\text{Precision}(L, F, E, R) + \text{Recall}(L, E, R)}$$

The auditing system's objective is to select the reasons R to maximize the F-measure. In our case, a high F-measure is not sufficient to ensure the auditing system functions properly. That is, if the precision of the system is low, then even though many real accesses are explained, the utility of the system is minimal. Therefore, we also add an additional constraint that

the precision must be greater than a minimum threshold (eg, precision ≥ 0.85).

For a fair analysis, the size of the fake log was explicitly set to the size of the real log. While the number of inappropriate accesses is smaller than the number of appropriate accesses in practice, it would be unfair to measure the quality of the auditing system using a fake log that is significantly smaller than the real log. This configuration is unfair because the auditing system could simply classify each real and fake access as appropriate, even though the explanation is meaningless, and still attain near perfect precision and recall. Instead, with equally sized logs, the auditing system is forced to produce explanations that correctly explain real accesses without spuriously explaining fake accesses.

METHODS

Our hypothesis is that specific hospital employees are responsible for treating a diagnosis. Moreover, instead of acting independently, employees treat patients collaboratively. We leverage these observations to explain why accesses to medical records occur. That is, if the auditing system is confident that an employee is responsible for treating a diagnosis, then the associated accesses are appropriate. For example, consider the patient Alice who requires chemotherapy, and Dr Carl who works in the Hematology/Oncology (Hem/Onc) Department. The auditing system can explain why Dr Carl accessed Alice's medical record: Dr Carl accessed Alice's medical record because Hem/Onc employees are responsible for chemotherapy patients.

The challenge is then to determine which employees are responsible for each diagnosis and to quantify the confidence in this decision. The first part of this section examines this problem when departments treat a diagnosis, and the second part considers clustering similarly treated diagnoses.

Explaining accesses

Given a diagnosis, the objective is to determine the set of employees that are responsible for treating it. While it is possible to determine, at the granularity of individual employees, who is responsible for a diagnosis, we observe several limitations with this fine granularity. First, many employees treat the same diagnosis. For example, another doctor in the Hem/Onc Department could also adequately treat Alice. Second, hospitals typically schedule employees in shifts and rotations, where different employees are responsible for the same patients at different times. Therefore, analyzing treatment behavior at the granularity of individual employees suffers from noise.

Instead, we determine diagnosis responsibility information at the granularity of hospital-designated departments. Intuitively, these departments serve as a grouping of employees with similar responsibilities. Moreover, we can assume these groupings are relatively accurate because EMR administrators manage them. Interestingly, the specificity of the diagnoses a department treats varies greatly. In some cases, like the Hem/Onc Department, employees are responsible for specific types of diagnoses. In contrast, departments such as the Central Staffing Department (which contains nurses who rotate throughout the hospital based on need) treat a wide range of diagnoses. Hospital-designated departments are limited because they cannot be used to detect fine-grained inappropriate behavior such as when one employee from a department should be able to access a patient's record while another employee in the same department should not. However, given that employees in the same department often speak about patients during rounds, this level of abstraction seems to be a reasonable

compromise between the typical flow of information in a hospital and the expressivity of security policies. While previous work has used access patterns to construct collaborative groups to capture working relationships more accurately,⁹ these hospital-designated departments provide a natural starting point for defining employee groups that are interpretable and effective.

The objective can then be restated as: given a diagnosis, find the set of departments that are responsible for treating it. A simple metric is the likelihood that an employee from a department accesses the medical records of patients with the given diagnosis. The intuition is that if a department is responsible for a diagnosis, then it is highly likely that someone from the department will access the associated patients' records. For example, if we consider a chemotherapy patient, it is more likely that the Hem/Onc Department will access the patient's record than the Dermatology Department.

Definition 1 (Access probability) The access probability for a diagnosis c and a department d is defined as the probability that an employee in department d will access a patient's medical record, given that the patient has diagnosis c :

$$\text{AP}(\text{Department } d | \text{Diagnosis } c) = \frac{|\text{Patients with diagnosis } c \text{ accessed by department } d|}{|\text{Patients with diagnosis } c|}$$

One might consider using the access probability alone to conclude that a department d is responsible for diagnosis c (ie, if the access probability is greater than a given threshold, the auditing system would conclude that all accesses by employees of department d to the records of patients having diagnosis c are appropriate). However, this ignores an important problem: accesses by employees in general departments (eg, Central Staffing) would nearly always be deemed appropriate because employees in these departments are involved in broad aspects of patient care. While it is likely that someone from Central Staffing accesses each chemotherapy patient's record, it would be a mistake to conclude that Central Staffing is responsible for treating chemotherapy patients.

Observing these limitations, an additional metric is required to differentiate auxiliary accesses from accesses of employees that are responsible for treating a diagnosis. To this end, the treatment probability measures how likely it is that a patient has a specific diagnosis when employees from a given department access his medical record. The basic assumption here is that departments responsible for a diagnosis will have higher treatment probabilities because these departments treat a smaller and more narrow set of diagnoses than auxiliary departments (eg, Hem/Onc employees treat a smaller set of diagnoses than Central Staffing employees).

Definition 2 (Treatment probability) The treatment probability for a diagnosis c and department d is defined as the probability that an employee in department d is accessing a patient's medical record to treat diagnosis c :

$$\text{TP}(\text{Department } c | \text{Diagnosis } d) = \frac{|\text{Patients with diagnosis } c \text{ accessed by department } d|}{|\text{Patients accessed by department } d|}$$

A higher treatment probability indicates that the department is responsible for the diagnosis. For example, the treatment probability for the Hem/Onc Department to access a chemotherapy patient's medical record is much higher than the Central Staffing Department, even though Central Staffing employees frequently access chemotherapy patients.

The auditing system combines the probabilities to determine if a department is responsible for a diagnosis. In particular, if the access and treatment probabilities are above a threshold, the department is responsible for the diagnosis. Here, a responsible department implies that the department is specifically tasked to treat the diagnosis. It is important to note that while general diagnoses (eg, hypertension) are treated throughout the hospital, they are often not the responsibility of specific departments.

Ideally, a single pair of thresholds could be set to determine the responsible departments for all diagnoses. However, because the probabilities for each diagnosis have their own means and variances, responsibility information can be missed. For example, given $\text{TP}(\text{Chemotherapy} | \text{Hem/Onc}) = 0.12$, $\text{TP}(\text{Chemotherapy} | \text{Central Staffing}) = 0.05$, and $\text{TP}(\text{Strep Throat} | \text{Pediatrics}) = 0.01$, selecting a single threshold such that the Hem/Onc Department, but not Central Staffing, is responsible for chemotherapy, while the Pediatrics Department is responsible for strep throat, is not possible. Instead, the probabilities are normalized (denoted AP_N and TP_N) to a mean of zero and unit variance. (The access probability is normalized as follows: let $V_c = \{\text{AP}(d_1 | c), \dots, \text{AP}(d_N | c)\}$, $m = \text{mean}(V_c)$, $\text{std} = \text{stddev}(V_c)$, then $\text{normalized}(V_c) = \{(\text{AP}(d_1 | c) - m) / \text{std}, \dots, (\text{AP}(d_N | c) - m) / \text{std}\}$.) Thresholding the normalized access and treatment probabilities allows the auditing system to find responsible departments across all diagnoses with a single pair of thresholds. Moreover, thresholding the normalized probabilities provides for a relative comparison between the departments, so that responsible departments can be found even if the probabilities are small. As a result, this methodology finds responsible departments that have relatively larger access and treatment probabilities than other departments in the hospital.

More formally, responsibility is defined as follows:

Definition 3 (Responsibility) Given a diagnosis c , department d is responsible for the diagnosis if both of the following are true:

- The department frequently treats the diagnosis: $\text{AP}_N(d | c) \geq s$
- The department is directly involved in the diagnosis' treatment: $\text{TP}_N(c | d) \geq t$

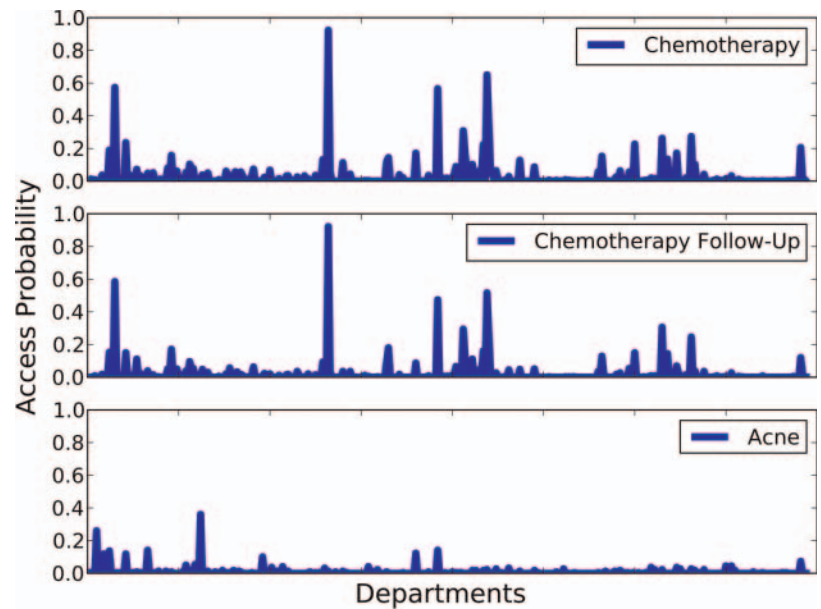
Where s and t are thresholds specified by the compliance officer.

Recall from the objective section, the EBAS is provided with a set of reasons for access as input. For our purposes, the set of reasons that are input to the auditing system include departmental responsibility information and direct explanations from the EMR database (eg, patient appointments, visits, medications, etc.).⁶ Alternative clinical and operational reasons are possible and we plan to study them in future work.

Definition 4 (Reasons for access) Consider an audit log entry describing the employee who accessed the medical record and the patient whose record was accessed. The patient is diagnosed with a set of diagnoses C . The EMR database also stores direct explanations using appointment, visit and medication information, among others. The access is appropriate if one of the following is true:

Research and applications

Figure 2 Access patterns for the diagnoses chemotherapy and follow-up chemotherapy are highly correlated compared to the access patterns for acne. The most likely department to access chemotherapy patients is the Cancer Center, while the most likely department for acne patients is dermatology. This figure is only reproduced in colour in the online version.



- The employee is assigned to a department that is responsible for treating one of the patient's diagnoses.
- The EMR database stores direct explanations describing the reason for access.

Overfitting diagnoses

As described above, the auditing system attempts to determine which departments are responsible for a given diagnosis. However, in many cases, multiple diagnoses (with unique ICD-9 codes) require the same or similar treatment. For example, 'encounter for antineoplastic chemotherapy' and 'follow-up examination following chemotherapy' (with ICD-9 codes V58.11 and V67.2, respectively) require similar treatments. Due to these similarities, the auditing system can potentially overfit the responsibility information.

Our observation is that if diagnoses with similar treatments are clustered, and the access and treatment probabilities are calculated using all diagnoses in the cluster, then the resulting responsibility information is more representative of actual clinical processes. More formally, we construct diagnosis clusters in the following manner: let the patient vector $\mathbf{V}_p$ be a boolean vector of length N , where N is the number of departments. Index i is set to 1 (ie, $\mathbf{V}_p(i)=1$) if an employee from department i accessed patient p 's medical record, and 0 otherwise. A diagnosis vector $\mathbf{V}_c$ is the average of all patient vectors when the patient has diagnosis c . The resulting values represent the access probabilities for each department. We say two diagnoses c_i and c_j are treated similarly if their vectors' Pearson's correlation coefficient is greater than a provided threshold. More formally, two diagnoses are clustered if $\text{corr}(\mathbf{V}_{c_i}, \mathbf{V}_{c_j}) \geq v$, where $v=1.0$ implies no clustering and smaller values of v increase the number of diagnoses clustered. As figure 2 shows, chemotherapy and follow-up chemotherapy have highly correlated treatments (Pearson's correlation coefficient of 0.97) compared to acne.

DATA

We conducted an extensive experimental study using data from the University of Michigan Health System. The dataset contains a de-identified audit log consisting of 4.5 million accesses during a week by 12 000 employees from 291 departments to

124 000 patients' medical records. The accesses in the log can be divided into two groups: first accesses (ie, accesses in which an employee accesses a patient's medical record for the first time in the log), and repeat accesses. The dataset also contains evidence describing the reason for access such as diagnosis, appointment, visit, and medication information, among others listed in table 1. It is important to note that our dataset is a temporal snapshot of the EMR database from the weeks around the accesses in the audit log. As a result, information such as diagnoses and appointments outside this snapshot were not reported for our study. This directly impacts the number of diagnoses that we were provided (we have diagnoses for approximately 47% of the patients).

For the evaluation, we divide the patients for which we have diagnoses into two sets: a training set and a testing set. The training set and testing set each contain approximately 29 000 patients and 200 000 real and fake first accesses to these patients' medical records. The access and treatment probabilities are calculated using only real first accesses for patients in the training set to determine the responsible departments.

Table 1 Data overview

Log characteristic	Value
No. of employees	12 000
No. of departments	291
No. of patients	124 000
No. of patients with diagnoses	58 000
Evidence	No. of records
Audit log accesses	4.5 million
Audit log first accesses	509 000
Appointments (outpatient)	51 000
Diagnosis instances (ICD-9)	248 000
Documents	76 000
Inpatient medications	122 000
Labs	45 000
Outpatient medications	120 000
Radiology orders	17 000
Services/orders	106 000
Visits (inpatient)	3000

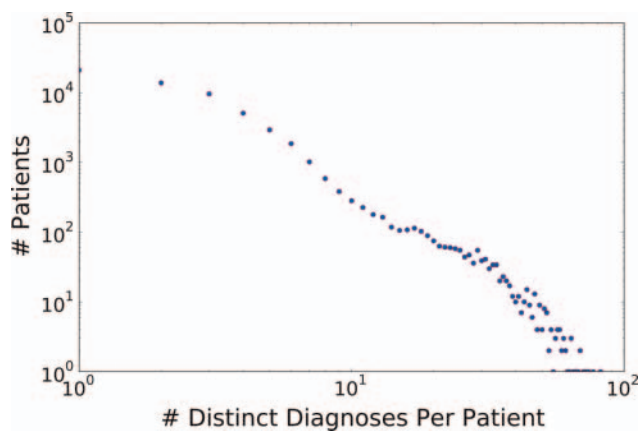


Figure 3 Diagnoses per patient: patients on average have three diagnoses, but the distribution has a long tail. This figure is only reproduced in colour in the online version.

We only consider diagnoses that occur at least 30 times. The reasons for access are then evaluated on real and fake first accesses for patients in the testing set to calculate the recall, precision and F-measure.

To provide more insight into the diagnosis information, figure 3 shows that patients on average have three distinct diagnoses, but the distribution is heavily skewed ('long-tail'). When a patient has multiple diagnoses, the auditing system does not know which accesses correspond to each diagnosis. Figure 4 shows that the number of distinct accesses to a patient's medical record (ie, distinct patient-employee pairs in the real audit log) is positively correlated with the number of distinct diagnoses for the patient (Pearson's correlation coefficient of 0.74).

RESULTS AND DISCUSSION

The first question we aim to answer is whether the auditing system produces semantically correct responsibility information for a given diagnosis. Table 2 shows the system's output for selected diagnoses and departments. For example, the departments that are likely to treat patients who require a kidney transplant are the Nephrology Department and Transplant Center. The Cancer Center and Hem/Onc Department are responsible for chemotherapy patients. In contrast, even though the Central Staffing Department accesses a majority of

chemotherapy patients' records, the normalized treatment probability is low because the department treats a wide range of diagnoses.

Next, we analyze the impact of the access and treatment probability thresholds on precision and recall for a few selected diagnoses. Figure 5 shows the results when accesses are explained using the responsibility information for a given diagnosis, without direct explanations, as the normalized treatment probability threshold is varied and the normalized access probability threshold is held constant. For these figures, recall for a single diagnosis is 1.0 when all accesses for patients with the diagnosis are explained, and recall increases as more departments are determined to be responsible for a diagnosis. As expected, higher treatment thresholds produce better precision at the cost of lower recall. The precision drops to 60% for low treatment probability thresholds, but plateaus because of the minimum access probability required (ie, figure 5(C)). Interestingly, general diagnoses such as hypertension have few if not any responsible departments due to their low normalized treatment probabilities because these diagnoses occur across every department. For example, hypertension has no responsible departments for thresholds larger than $s=1.0$ and $t=2.0$, which produces a recall of zero for the diagnosis (ie, figure 5(D)). As a result, for higher thresholds, general diagnoses are not as effective at explaining why accesses occur compared to more specific diagnoses such as kidney transplant. Future work is needed to explain accesses for diagnoses that are encountered throughout the hospital.

Table 3 shows the recall, precision and F-measure for various thresholds when all reasons for access are aggregated (ie, the set of accesses explained by the disjunction of reasons). As shown in previous work, direct explanations have a recall of 22% with near perfect precision.⁶ The high precision is due to the sparsity of employee-patient relationships, which makes it unlikely that a fake access corresponds to actual evidence. As responsibility information is included, two times as many first accesses are explained at the cost of lower precision (eg, 41% recall with 90% precision for $s=1.0$ and $t=2.0$). In addition to the recall, precision and F-measure, table 4 further breaks down the results by the number of real and fake accesses that are explained and unexplained, respectively. The responsibility information introduces a drop in precision because it is at the granularity of a department instead of an individual employee. Clustering similarly treated diagnoses focuses the auditing system on the departments that are responsible for a diagnosis and provides a slight improvement in precision. For example,

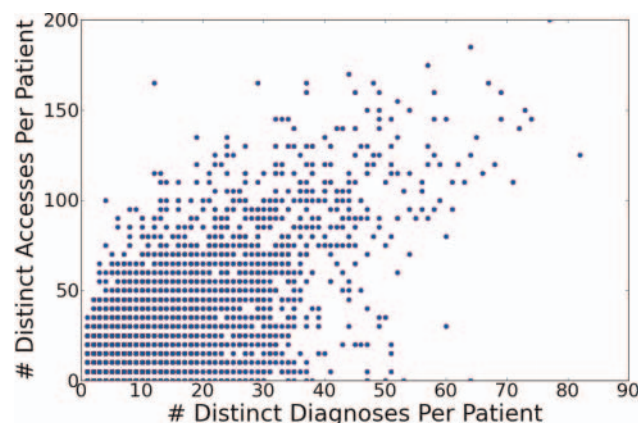


Figure 4 Access-diagnosis correlation: the number of distinct accesses for a patient is correlated with the number of distinct diagnoses for the patient. This figure is only reproduced in colour in the online version.

Research and applications

Table 2 Normalized access and treatment probabilities for selected departments and diagnoses

Chemotherapy			Kidney transplant			Strep throat		
Department	AP _N (AP)	TP _N (TP)	Department	AP _N (AP)	TP _N (TP)	Department	AP _N (AP)	TP _N (TP)
Cancer Center	9.19 (0.91)	1.00 (0.12)	Transplant	8.14 (0.56)	5.61 (0.20)	Pediatrics	14.04 (0.64)	6.25 (0.019)
Pharmacy	6.52 (0.66)	1.38 (0.16)	Nephrology	6.21 (0.43)	6.22 (0.23)	Central Staff	4.41 (0.21)	0.94 (0.004)
Central Staff.	5.54 (0.56)	0.24 (0.06)	Pharmacy	2.78 (0.21)	0.20 (0.02)	Health Cntr.	3.17 (0.11)	2.69 (0.009)
Hem/Onc	5.54 (0.56)	2.07 (0.21)	Dialysis	1.11 (0.10)	2.91 (0.11)	Nursing-ER	1.30 (0.07)	1.75 (0.006)
Nursing-Hem/Onc	2.98 (0.32)	2.20 (0.23)	Nursing-Renal	1.02 (0.09)	2.04 (0.08)	Family Med.	0.99 (0.05)	0.27 (0.002)

The probabilities are normalized to a zero mean and unit variance so that values are comparable across diagnoses.

after clustering, various nursing departments are no longer thought to be responsible for chemotherapy. In summary, the EBAS filters a large subset of the first accesses and over 94% of all accesses (when repeat accesses are filtered).

Finally, table 5 lists which departments account for the largest proportion of unexplained first accesses, and the rate at which a department's accesses are unexplained. As expected, departments that provide wide ranges of services throughout the hospital (eg, Radiology and Central Staffing) are often unexplained, even though these general departments access most patients' medical records. In contrast, departments that provide narrow sets of services such as the Allergy, Neonatology, Dermatology, Nephrology and Thoracic Surgery Departments have unexplained rates that are equal to or less than 0.05. This is not to say that Central Staffing employees are more likely to access records inappropriately. However, we

cannot use diagnosis information to explain why their accesses occur. Future work is needed to explore alternative types of explanations to remedy this gap in the auditing system for general departments.

RELATED WORK

Anomaly detection systems have been studied extensively in the past.¹⁰ For EMR, Chen and colleagues^{9–11} study the extent to which employee access patterns deviate from their peers to detect inappropriate use. Boxwala *et al*¹² extract patient–employee relationships, patient characteristics, and employee characteristics that are used as features in various classifiers to detect suspicious accesses. While our work focuses on data available within the EMR database, other work considers aggregating external data sources to improve auditing.¹³

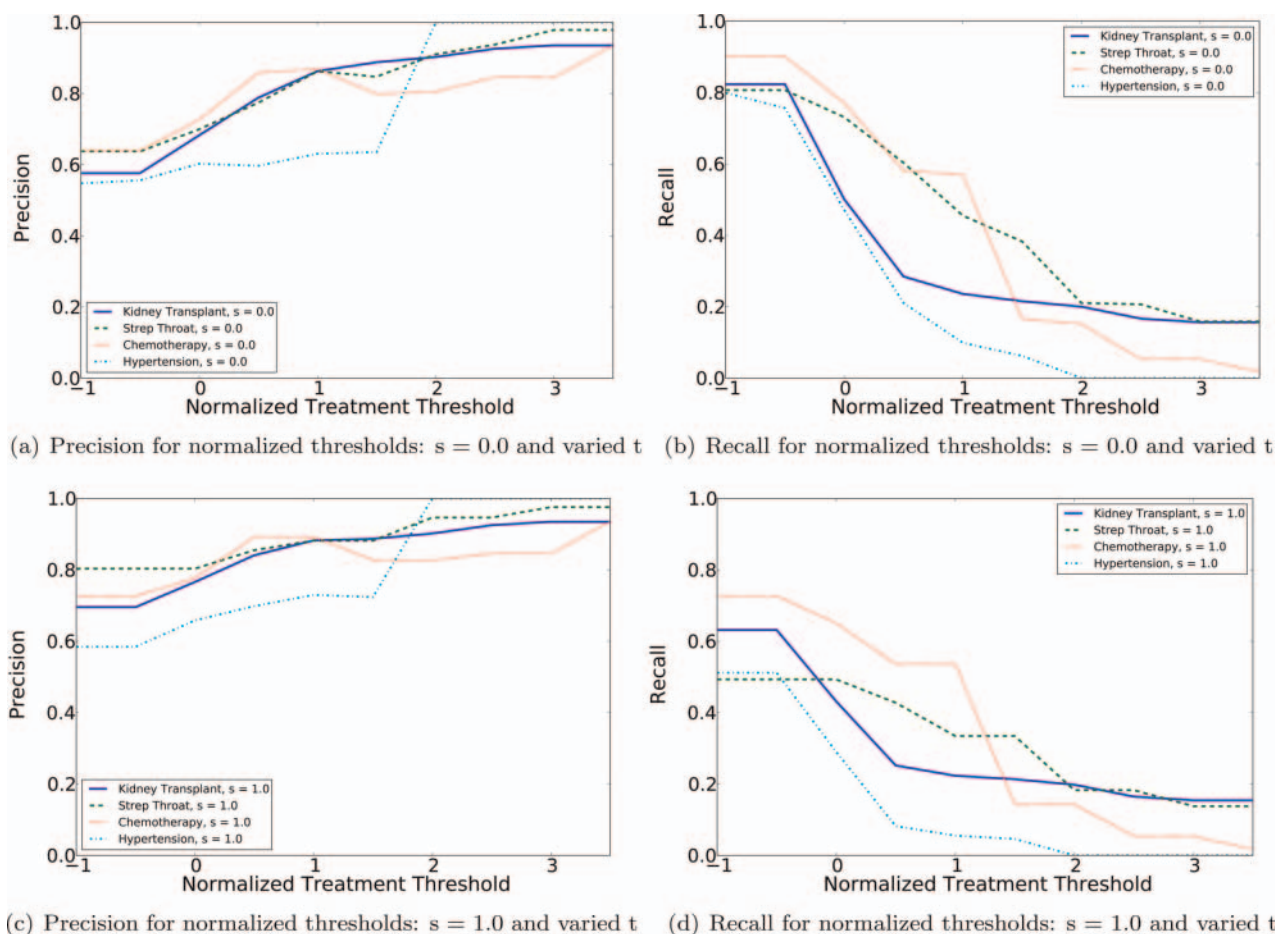


Figure 5 Recall and precision when explaining accesses using only selected diagnosis responsibility information (s=Normalized access probability threshold, t=Normalized treatment probability threshold). This figure is only reproduced in colour in the online version.

Table 3 Aggregate results for all diagnoses with varying thresholds (s=normalized access probability threshold, t=normalized treatment probability threshold, v=clustering threshold)

Description	s	t	v	Recall	Precision	F-Measure
Evidence+responsibility	1	1	1.00	0.534	0.830	0.650
Evidence+responsibility+clustering	1	1	0.95	0.540	0.842	0.658
Evidence+responsibility+clustering	1	1	0.90	0.529	0.856	0.654
Evidence+responsibility	1	2	1.00	0.411	0.904	0.565
Evidence+responsibility+clustering	1	2	0.95	0.419	0.915	0.574
Evidence+responsibility+clustering	1	2	0.90	0.411	0.920	0.568
Evidence+responsibility	1	3	1.00	0.344	0.945	0.504
Evidence+responsibility+clustering	1	3	0.95	0.353	0.953	0.515
Evidence+responsibility+clustering	1	3	0.90	0.353	0.957	0.515
Evidence only	—	—	—	0.229	0.997	0.372

Table 4 Confusion matrix (for s=1.0, t=2.0, v=1.0) shows the breakdown of first accesses explained

	Explained	Unexplained
Real first accesses	80 000	115 000
Fake first accesses	8000	187 000

Table 5 Departments with the most unexplained first accesses (for s=1.0, t=2.0, v=1.0).

Department	Unexplained rate	Proportion of all unexplained first accesses
Cancer center	0.78	0.08
Radiology	0.90	0.07
Central staffing	0.86	0.05
Physician services	1.00	0.04
General medicine	0.21	0.04
Outpatient services	0.82	0.04
Pharmacy	0.88	0.04
Health info. management	0.98	0.04

In some sense, using diagnosis information to explain why accesses occur is related to previous work on mining workflows.¹⁴ Similar to determining who is expected to treat a patient, Russello *et al*¹⁵ propose an access control framework for e-Health that adapts access rights to the actual tasks employees have to fulfill. Similarly, experience-based access management systems attempt to understand medical record usage under a probabilistic framework to construct relational access control policies to better predict employee data needs.^{16–18} Limiting access in hospitals is often difficult because patient treatment is dynamic. To provide exceptions to access control policies, previous work has evaluated if allowing employees to escalate their permissions would provide a reasonable compromise (these escalated accesses are specially logged and reviewed). Unfortunately, employees escalated their permissions for over 50% of the patients.¹⁹

Hospital-designated departments serve as a natural grouping of employees based on shared roles and responsibilities. However, assigning thousands of employees to these departments is a difficult challenge. To automate this process, recent work has examined predicting an employee's department or role using EMR audit logs.²⁰ These roles have the potential to be used in a role-based access control system if highly accurate.²¹

In this work we assume that the ICD-9 diagnosis codes are correctly entered. However, errors are possible. Recent work has

analyzed medical record text to predict the patient's ICD-9 code.²² Moreover, patients are often diagnosed with many related conditions. Patnaik *et al*²³ mine temporal sequences of diagnoses to understand better their correlation and temporal relationships.

CONCLUSION

This work considers the problem of ensuring the security and appropriate use of the patient health information stored in EMR. We presented an addition to the EBAS that determines which employees are responsible for treating a given diagnosis. This new class of explanation is used to filter appropriate accesses that occur for valid clinical or operational reasons, resulting in a smaller number of accesses for the compliance officer to review manually. An extensive evaluation using data from the University of Michigan Health System demonstrates that patient diagnosis information increases the number of first accesses explained by a factor of two over previous work and explains over 94% of all accesses with high precision.

Funding This work was supported by National Science Foundation grants CNS-0915782 and IGERT-0903629.

Contributors DF performed the problem formulation, system development, evaluation and interpretation of the experiments, and writing of the manuscript. KL performed the problem formulation, design and interpretation of the experiments, and writing of the manuscript. All authors read and approved the final manuscript.

Competing interests None.

Ethics approval This study received ethics approval from the University of Michigan Institutional Review Board.

Provenance and peer review Not commissioned; externally peer reviewed.

REFERENCES

1. Hensley S. Snooping Tucson hospital workers fired in records breach. <http://www.npr.org/blogs/health/2011/01/14/132928883/snooping-tucson-hospital-workers-fired-in-records-breach> (accessed 25 March 2012).
2. Ornstein C. Hospital to punish snooping on Spears. *Los Angeles Times*, 2008.
3. Cotter B. Peeking at medical records an issue for health centers. *Colorado Springs Gazette*, 2011.
4. Ferreira A, Cruz-Correia R, Antunes L, *et al*. Access control: how can it improve patients healthcare? *Stud Health Technol Inform* 2007;**127**:65–76.
5. Fabbri D, LeFevre K. Explanation-based auditing. *PVLDB* 2011;**5**:1–12.
6. Fabbri D, LeFevre K, Hanauer DA. Explaining accesses to electronic health records. *Proceedings of the 2011 Workshop on Data Mining for Medicine and Healthcare*, 2011:10–17.
7. Asaro PV, Herting RL, Roth AC, *et al*. Effective audit trails—a taxonomy for determination of information requirements. *AMIA* 1999:663–5.
8. Salazar-Kish J, Tate D, Hall PD, *et al*. Development of CPR security using impact analysis. *AMIA* 2000:749–53.
9. Chen Y, Malin B. Detection of anomalous insiders in collaborative environments via relational analysis of access logs. *CODASPY* 2011:63–74.
10. Chandola V, Banerjee A, Kumar V. Anomaly Detection: A Survey. *ACM Compu Surv* 2009;**41**.

Research and applications

11. **Chen Y**, Nyemba S, Zhang W, *et al*. Specializing network analysis to detect anomalous insider actions. *Secur Inform* 2012;**1**:1–24.
12. **Boxwala AA**, Kim J, Grillo JM, *et al*. Using statistical and machine learning to help institutions detect suspicious access to electronic health records. *JAMIA* 2011;**18**:498–505.
13. **Herting R Jr**, Asaro P, Roth A, *et al*. Using external data sources to improve audit trail analysis. *AMIA* 1999:795–9.
14. **van der Aalst W**, Vandongen B, Herbst J, *et al*. Workflow mining: a survey of issues and approaches. *Data Knowledge Eng* 2003:237–67.
15. **Russello G**, Dong C, Dulay N. A workflow-based access control framework for e-health applications. 22nd International Conference on Advanced Information Networking and Applications – Workshops, 2008;111–20.
16. **Gunter CA**, Liebovitz DM, Malin B. Experience-based access management: a life-cycle framework for identity and access management systems. *IEEE Secur Privacy* 2011;**9**:48–55.
17. **Li X**, Xue Y, Malin B. Towards understanding the usage pattern of web-based electronic medical record systems. *IEEE International Symposium on a World of Wireless. Mobile and Multimedia Networks*, 2011;1–7.
18. **Malin B**, Nyemba S, Paulett J. Learning relational policies from electronic health record access logs. *J Biomed Inform* 2011;**44**:333–42.
19. **Rostad L**, Edsberg O. A study of access control requirements for healthcare systems based on audit trails from access logs. *Computer Security Applications Conference* 2006:175–86.
20. **Zhang W**, Gunter CA, Liebovitz D, *et al*. Role prediction using electronic medical record system audits. *Proceedings of the 2nd USENIX conference on Health security and privacy*, 2011.
21. **Sandhu RS**, Coyne EJ, Feinstein HL, *et al*. Role based access control models. *IEEE Comput* 1996;**29**:38–47.
22. **Yan Y**, Fung G, Dy JG, *et al*. Medical coding classification by leveraging inter-code relationships. *International Conference on Knowledge Discovery and Data Mining*, 2010:193–202.
23. **Patnaik D**, Butler P, Ramakrishnan N, *et al*. Experiences with mining temporal event sequences from electronic medical records: initial successes and some challenges. *KDD* 2011:360–8.



Explaining accesses to electronic medical records using diagnosis information

Daniel Fabbri and Kristen LeFevre

J Am Med Inform Assoc 2013 20: 52-60 originally published online November 2, 2012
doi: 10.1136/amiajnl-2012-001018

Updated information and services can be found at:
<http://jamia.bmj.com/content/20/1/52.full.html>

These include:

References

This article cites 7 articles, 1 of which can be accessed free at:
<http://jamia.bmj.com/content/20/1/52.full.html#ref-list-1>

Email alerting service

Receive free email alerts when new articles cite this article. Sign up in the box at the top right corner of the online article.

Notes

To request permissions go to:
<http://group.bmj.com/group/rights-licensing/permissions>

To order reprints go to:
<http://journals.bmj.com/cgi/reprintform>

To subscribe to BMJ go to:
<http://group.bmj.com/subscribe/>