Development of CPR Security Using Impact Analysis

Jolin Salazar-Kish, PhD; Dawn Tate, MS; Priscilla D. Hall, MS, RN,C; Karen Homa, MS
Department of Clinical Computing
Dartmouth-Hitchcock Medical Center, Lebanon, New Hampshire

Abstract
The HIPAA regulations will require that institutions ensure the prevention of unauthorized access to electronically stored or transmitted patient records. This paper discusses a process for analyzing the impact of security mechanisms on users of computerized patient records through "behind the scenes" electronic access audits. In this way, those impacts can be assessed and refined to an acceptable standard prior to implementation. Through an iterative process of design and evaluation, we develop security algorithms that will protect electronic health information from improper access, alteration or loss, while minimally affecting the flow of work of the user population as a whole.

Introduction
As the use of technology in health care grows, so does public unease around the issues of patient privacy and the misuse of patient health records. As a result, the Health Insurance Portability and Accountability Act (HIPAA) incentives are mandating the enactment of federal laws and regulations against unauthorized access to electronically stored or transmitted patient records and misuse of personal health information. Healthcare institutions are responding by reviewing existing security policies and procedures and working to develop strategies that will enable them to sensibly manage patient information.

A review of the literature shows a significant number of articles related to security and confidentiality of patient health care information. Many of these address proposed regulations and/or legislation related to HIPAA mandates[1-3], to general rights, responsibilities, principles, and standards[4-7], or to security related to a particular aspect of the field of health care information such as telemedicine[8] or web based systems[9-12]. Strategies for meeting today's complex requirements are less in evidence. Audits and audit analysis are examined in a number of articles[13,14], as is the "scrubbing" or removal of identifiable patient information from text[15,16]. Role based access has also been addressed[17,18]. Strategies for identification of a patient-provider relationship are examined in one study[19]. Another article describes a mechanism for asking the user accessing patient information for the first time to declare a reason for doing so[20].

The HIPAA regulations focus on three major areas for attaining security in a Computer-based Patient Records system:

1. Provide sufficiently anonymous release of information for research purposes.
2. Provide appropriate controls to prevent unauthorized people from gaining access to an organization's information systems (the infrastructure) and control of external communications links and access (the network).
3. Provide mechanisms for controlled and user-differentiated access to individual patient records.

The third item – restricting access to specific patient data based on a user's role and need to know – is the focus of this paper. We examine the process of designing a security algorithm that will protect electronic health information from improper access, alteration or loss while minimally affecting the flow of work of the user population as a whole.

Background
Dartmouth-Hitchcock Medical Center (DHMC) is an integrated care delivery system providing primary through tertiary care in New Hampshire and Vermont. It includes The Dartmouth-Hitchcock Clinic, The Dartmouth-Hitchcock Alliance and Dartmouth Medical School. At Dartmouth-Hitchcock, an integrated paper record (ambulatory and inpatient) has existed for more than 70 years.

The Clinical Information System (CIS) used throughout the Dartmouth-Hitchcock healthcare system is the product of an internal systems development effort. CIS accesses and displays data from several different source systems in one interface. These systems include several IDX applications such as Patient Registration, ADT, Scheduling, Radiology, Managed Care and Patient Billing for both hospital and professional based charges. Other systems in use include Cerner Laboratory, Pharmacy and Respiratory. CIS also provides features for workflow management and direct data entry by clinicians including medications allergies and notes.

1067—5027/00/$5.00

Currently, patient record security at DHMC has been provided through several mechanisms. These include confidentiality education and agreements, use of password and user name, use of the Kerberos network authentication protocol[21,22], review of audits, employee access to audit trails of their own records, and patient ability to request an audit of who has accessed their records (electronic or paper).

Methodology

Our challenge is to design a security scheme that will minimize unauthorized electronic access to patient data while maximizing user confidence in the system and ease of use. A robust security system allows medical professionals to access information with both a need to know, and with a right to know, but no access to those who do not. The goal is to develop a security system that balances the needs of the users (providing medical care) with the needs of the patient (medical record privacy).

The DHMC Clinical Information System currently grants full access to all patient data to all providers in our network. As we implement a security system, we recognize the need for phased implementation to avoid any interruptions in the provision of patient care. Our approach is as follows:

1. Develop algorithms for determining appropriate access to electronic patient records using available User-Patient relationship data.
2. Develop refinements to the security mechanism to optimize the ordering of the algorithmic checks, the timeframes around which to look for user-patient relationships, and to minimize impact on those identified special user populations.
3. Programmatically monitor and analyze how the algorithm's implementation would have affected users of the system if we were to use those User-Patient relationships as a basis for limiting access.
4. Repeat steps 2-4.

In order to provide the level of security required for HIPAA compliance, a mechanism for determining a User-Patient relationship using data available in CIS is necessary. If a relationship cannot be identified, a user would be issued a warning and requested to either 1- enter a reason for continuing, or 2- exit. In some cases, it may also be appropriate to deny access to a patient record if no user-patient relationship can be determined by the system.

In order to monitor how the mechanism's implementation will affect users of the system, we implemented our security algorithm such that instead of actually issuing a warning and asking for an access reason, it simply keeps a log of the times that the warning would have been issued. A sample of 50 medical professionals was selected for testing. Within a 20-day period, a total of 17,243 patient medical records were viewed. Each medical professional viewed between 3 and over 2,500 medical records during that time. Of the users in our sample, 33 were doctors, 13 were registered nurses, and one was a LPN, and one user was a physical therapist.

Thus, we approached the design process as one of iterative refinement. We are attempting to anticipate user needs by measuring the impact of our proposed security system on the user community before we are required to turn it on. With proper design and analysis, we will have the information we need to inform the user community of the how the new security features will affect them.

Although it is our ultimate goal to entirely eliminate the possibility of a patient's data being misrepresented or misused for malicious intent, the potential for security breaches still exists. An extensive auditing system can provide a means for identifying users who have inappropriately accessed patient data. As part of our security system, therefore, we are building an auditing system that is both easy to use and to derive data from. Additionally, we will develop a policy for taking corrective action should an information breach occur.

Algorithm Development

Inherent in the concept of access control is the notion of a pre-existing relationship between the user and the patient. Therefore, our first step in designing a security mechanism is to examine our database to identify information that we currently store that can be used to signify a relationship between a user and a patient. By using information that is already available, we are deliberately choosing not to burden the user with the necessity of having to enter a reason every time they access a patient's record. We established the following six identifiers upon which we base a User-Patient relationship in our algorithm:

1. The user is the **Primary Care Physician**.
2. The user is the **Scheduled Provider**.
3. The user is the **Referring Provider** for the scheduled appointment.
4. The user is in the **same department** as the **Primary Care Physician**.
5. The user is in the **same department** as the **Scheduled Provider**.
6. The user is in the **same department** as the **Referring Provider** for the scheduled appointment.

Optimal Algorithmic Ordering

In order to implement the algorithm with optimal response time, it is essential that all the checks we make "behind the scenes" for User-Patient relationships are performed in the shortest time possible. Therefore, if we know which of our identifiers is most likely to determine a User-Patient 'match', then we should test for those identifiers first. If a 'match' is found in the first test, there is no need to continue testing, and no warning is issued. In this way, the order that the identifiers are tested within the security algorithm is optimized.

In order to determine the optimal ordering of the identifier tests, we need to determine those identifiers with the highest access permitted. Therefore, initially, all patient lookups are processed through each identifier test; this would not happen normally. Access rate per test is defined as the total number of medical records that are allowed access divided by the total number of medical records requested.

Optimal Access Time Window

The identifiers themselves fall into two categories: time independent and time dependent. Whether or not the user is the primary care physician (1) or in the same department as the primary care physician (4) is time independent. That is, either the user is the Primary Care Physician (or in the same department as the PCP) at the time of access, or not. For the other identifiers, however, we need to consider a window of time around an attempted access in which to look for a relationship based upon a scheduled appointment. If a user tries to access a medical record for a patient that has a scheduled appointment, and that appointment date lies outside of the established time frame, that user will be issued a warning and asked to enter a reason for accessing the record.

We must analyze the relationship between the date range allowed around a patient lookup and the frequency of the existence of a User-Patient relationship (termed a "match"). It is critical that we identify the optimal time window in which to search for a User-Patient relationship. If the amount of time we allocate is too small, the users will be unnecessarily encumbered. If the amount of time we allocate is too large, there will exist a potential for misuse of patient information. Using the identifiers above, we study the effects of length of time around a requested access on the likelihood of a match. We examine time ranges of 14-days to 6 months before and after the requested access.

User Impact Analysis

For each time range, we analyze actual lookups for our sample users. Impact rate is the measure of performance used for the algorithm. Impact rate is equivalent to the number of medical records that represent "unmatched" access divided by the total number of medical records the user was attempting to access. Impact rate is similar to mortality rate – the lower the value the better the result and the smaller the burden on the user.

Results

The results of our analysis of the optimal algorithmic ordering, access time window, and user impact are shown in Figures 1-3.

Optimal Algorithmic Ordering Results

The results of our examination of the optimal ordering of the User-Patient relationship identifiers are shown in Figure 1. For our sample of users, the optimal ordering is to check if the user is 1- a scheduled provider, 2- in the same department as the scheduled provider, 3- in the same department as the primary care physician, 4- in the same department as the referring provider, 5- a referring provider, or 6- a primary care provider.

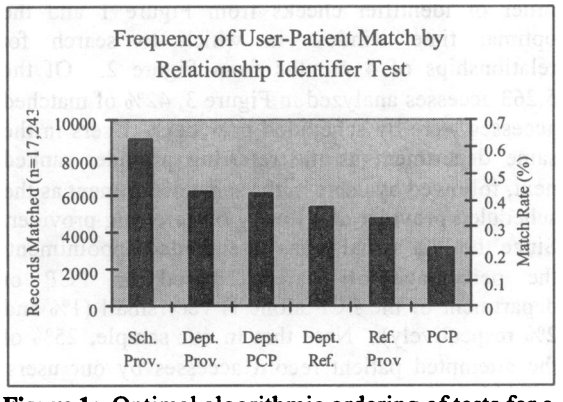

Figure 1: Optimal algorithmic ordering of tests for a User-Patient relationship.

Optimal Access Time Window Results

The results of our examination of the optimal time window in which to search for a User-Patient relationship are shown in Figure 2. The impact rate decreases steadily from 14 days to two months, and then begins to level off. It is important to note that whether we examine the overall impact rate, or the impact rate per relationship identifier, that the determination of the optimal time window remains the same. After four months, the additional access allowed by the algorithm by looking longer than four months on either side of the access request date for a User-Patient relationship is minimal. Therefore, we chose to four months as the optimal time frame. We used the four-month time window to determine the optimal algorithm order of tests for a User-Patient

relationship shown in Figure 1, and for all other analyses.

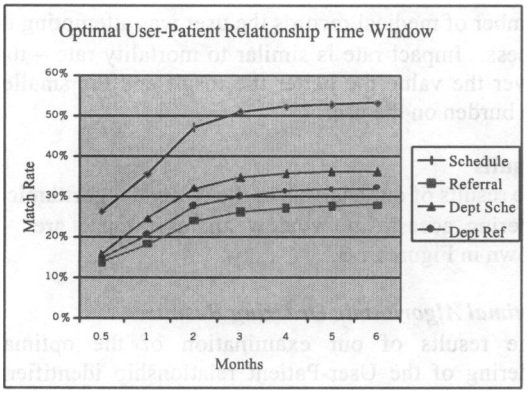

Figure 2: Optimal access time window to search for a User-Patient relationship.

User Impact Analysis Results

The results of our examination of the determinants of User-Patient relationships are shown in Figure 3. These data are obtained by using the optimal sort order of identifier checks from Figure 1 and the optimal time window in which to search for relationships of 4 months from Figure 2. Of the 5,263 accesses analyzed in Figure 3, 42% of matched accesses were by scheduled providers. Users in the same department as the referring provider ranked next, followed by users in the same department as the scheduled provider and finally by referring provider. Since the PCP usually has a scheduled appointment, the percentage of matches based on PCP or department of the PCP alone is very small (1% and 2% respectively). Note that in our sample, 25% of the attempted patient record accesses by our users would have resulted in the issuance of a warning (No Match category in Figure 3).

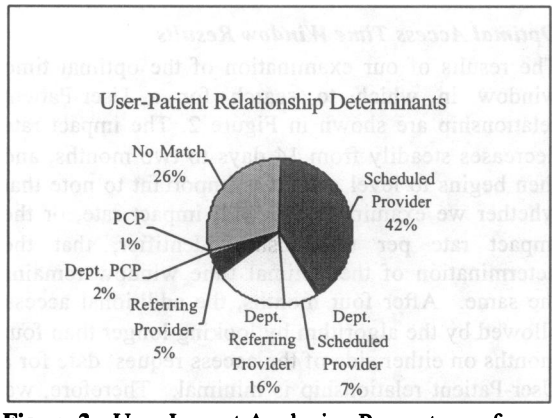

Figure 3: User Impact Analysis: Percentage of User-Patient relationships by identifier.

Discussion

This study has two aims: 1- to analyze the impact of a security algorithm on a set of CIS users and 2- to aid in the further development of that security algorithm. Using our four-month time window and optimal relationship identifier sort order in our security algorithm, the users in this sample would not be issued a warning in approximately 75% their attempts to access an electronic patient record. We feel that the 4-month time window is not excessively large or small from a clinical care point of view. However, we do not feel that it is acceptable for approximately a quarter of all accesses to result in a warning issuance interruption for our users (an impact rate of 26%).

To assess the access patterns, the impact rate was stratified by medical professional for the data in Figure 3, in order to assess stability over days. A p-chart analysis revealed instability in access patterns. With unstable access patterns, CIS security system developers cannot confidently inform users that turning on the security feature will have x impact on their daily work. The x is unknown due to the large usage variation for different medical professionals. Therefore, more detailed analysis of the population of users showing the greatest variation in access patterns and frequency of "no match" conditions is necessary before deploying this system.

Although the overall impact rate in this study is 26%, individual impact varies considerably for different medical professionals. Clearly, the impact rate does not represent simply snooping or human error. Medical professionals are accessing medical records that are not patients with scheduled appointments, or some medical professionals caring for a patient do not reside in the same department. We found that many of the "no match" cases were in response to patient phone calls. The task then, is to capture this other type of common User-Patient relationship in the CIS security system. In the second version of our algorithm, we will include additional checks such as "Is there a followup for this patient in the user's Worklist?" In this way, the person who answers the phone call will get the warning, but if they then put the item into the provider's worklist, the provider will not be issued a warning when accessing this patient.

Finally, if a warning is issued, our system tracks the patient, the time, the user, and the reason provided. It uses this information to generate a report that can be used by managers to verify appropriateness of access. We have been able to enhance this reporting feature by linking it to the Note writing feature in CIS. If a

provider has written a clinical electronic note (a permanent part of the electronic patient record) on the patient since the warned access, that access is then legitimized, and will not appear on the access tracking report that managers receive.

Conclusion

This research established a framework for systematically improving a security algorithm for access to computerized patient records. Using this methodology, any proposed changes to the security feature can be easily tested, in order to provide quantitative evidence of their effects on the impact rate. This framework and analysis strategy can be used to continuously improve the security algorithm.

Acknowledgement

The authors wish to thank Dennis O'Connor for providing programming support to capture the data used in these analyses.

References

1. Dunlay, CT. New rule helps ensure privacy of electronic medical records. Business First-Columbus 1999; 16(6):4a.
2. Hodge, JG, Gostin, LO, Jacobson, PD. Legal issues concerning electronic health information: Privacy, quality, and liability. J Am Med Assoc 1999; 282(15): 1466.
3. Appelbaum, PS. Threats to the confidentiality of medical records – no place to hide. J Am Med Assoc 1999; 283(6): 795.
4. Chilton, L, Berger, JE, Melinkovich, P, et al. Privacy protection and health information: patient rights and pediatrician responsibilities. Pediatrics 1999; 104(4 Pt. 1): 973-7.
5. Gritzalis, DA. Enhancing security and improving interoperability of healthcare information systems. Medical Informatics 1998; 23(4): 309-23.
6. Buckovich, SA, Rippen, HE, Rozen, MJ. Driving toward guiding principles: A goal for privacy, confidentiality, and security of health information. J Am Med Inform Assoc 1999; 6(2): 122-33.
7. Barrows, RC, Clayton, PD. Privacy, confidentiality, and electronic medical records. J Am Med Inform Assoc 1996; 3(2): 139-48.
8. Raman, RS, Reddy, R, Reddy, VJS, Cleetus, KJ, Srinivas, K. A strategy for the development of secure telemedicine applications. In: Masys DR, editor. Proc AMIA Annu Fall Symp 1997: 677-81.
9. Masys, DR, Baker, DB. Patient-Centered Access to Secure Systems Online (PCASSO): A secure approach to clinical data access via the World Wide Web. In: Masys DR, editor. . Proc AMIA Annu Fall Symp 1997: 340-3.
10. Halamka, JD, Safran, C. Virtual consolidation of Boston's Beth Israel and New England Deaconess Hospitals via the World Wide Web. In: Masys DR, editor. Proc AMIA Annu Fall Symp 1997: 349-53.
11. Myers, DL, Culp, KS, Miller, RS. Use of a web-based process model to implement security and data protection as an integral component of clinical information management. In: Lorenzi, NM, editor. Proc AMIA Annu Fall Symp 1999: 897-9.
12. Hripcsak, G, Cimino, JJ, Sengupta, S, WebCIS: Large scale deployment of a web-based clinical information system. In: Lorenzi, NM, editor. Proc AMIA Annu Fall Symp 1999: 804-8.
13. Asaro, PV, Herting, RL, Roth, AC, Barnes, MR. Effective audit trails – a taxonomy for determination of information requirements. In: Lorenzi, NM, editor. Proc AMIA Annu Fall Symp 1999: 663-5.
14. Herting, RL, Asaro, PV, Roth, AC, Barnes, MR. Using external data sources to improve audit trail analysis. In: Lorenzi, NM, editor. Proc AMIA Annu Fall Symp 1999: 795-9.
15. Sweeney, L. Guaranteeing anonymity when sharing medical data, the Datafly System. In: Lorenzi, NM, editor. Proc AMIA Annu Fall Symp 1999: 51-5.
16. Wang, JZ, Wiederhold, G. System for efficient and securre distribution of medical images on the internet. Proc AMIA Annu Fall Symp 1998:907-11.
17. Brannigan, VM. A framework for "need to know" authorizations in medical computer systems: Responding to the constitutional requirements. In: Ozbolt, JG, editor. Proc Annu Symp Comp App Med Care 1994: 392-6.
18. Dargahi, R, Classen, DW, Bobroff, RB, et al. The development of a data security model for the collaborative social and medical services system. In: Ozbolt, JG, editor. Proc Annu Symp Comp App Med Care 1994: 349-53.
19. Bowen, JW, Klimczak, JC, Ruiz, M, Barnes, M. Design of access control methods for protecting the confidentiality of patient information in networked systems. In: Masys DR, editor. Proc AMIA Annu Fall Symp 1997: 46-50.
20. Rind, DM, Wald, JS, Safran, C. Enhancing confidentiality in a clinical information system.Cimino, JJ, editor. Proc AMIA Annu Fall Symp 1996: 848.
21. http://www.isi.edu/gost/info/Kerberos/
22. Neuman, B, Ts'o, T. Kerberos: An authentication service for computer networks, IEEE Communications, September 1994; 32(9): 33-8.