A FRAMEWORK FOR "NEED TO KNOW" AUTHORIZATIONS IN MEDICAL COMPUTER SYSTEMS: RESPONDING TO THE CONSTITUTIONAL REQUIREMENTS

Vincent M. Brannigan, J.D.
Professor, Law and Technology
University of Maryland at College Park
College Park, MD 20742
(301) 405-6667 vb15@umail.umd.edu

"Need to Know" systems which restrict access to computerized data to those with a specified need for the data have been described as part of the solution to the problem of privacy in health care information systems. However, no operational "need to know" system is described in the medical literature. Recent legal developments in constitutional privacy protection make a "need to know" system mandatory, not optional. In sophisticated information systems users can utilize the unique characteristics of the system itself to implement a high level"need to know" system, based on the institution's own patient treatment pattern. This article provides an analytical tool for helping to define a "need to know" system with reference to the specific problems of health care institutions.

INTRODUCTION

There is widespread agreement among health care policymakers that computerized medical data should be restricted on a "need to know" basis.[9,14] Such a system would be required by the Fair Health Information Practices Act now before Congress.[10] Limiting access to those with a "need to know" has been adopted as a policy by the British Medical Association. [13] Ethics scholars have indicated that any use of patient data without consent must be based on some substantial need for the information,[11] and clinicians have recognized "need to know" as the proper automated implementation of the Hippocratic oath. [7]

Despite these pronouncements, some organizations persist in avoiding the process of effectively determining who should have access to medical data.[12] Some institutions claim to have a "need to know" system but simply assume that everyone on the staff needs to know everything about every patient, or assume that audit trails will identify privacy invaders so they can be held "responsible". However these approaches do not comply with the current developments in the law of privacy.

A series of legal decisions have defined protection for patient's privacy rights. The most important recent decision on medical privacy is Doe v. New York, where the United States Court of Appeals found that individuals have a constitutional right of privacy in data concerning HIV status.

> **"Individuals who are infected with the HIV virus clearly possess a constitutional right to privacy regarding their condition.... There is, therefore, a recognized constitutional right to privacy in personal information.[6]**

While the Court of Appeals cited the well known Supreme Court case of Whalen v. Roe it clearly went beyond Whalen in defining the constitutional right of privacy.

Restriction of data access to the smallest number of persons possible has ben one of the major concepts of constitutional privacy analysis. In Whalen the Supreme Court specifically noted that the data was available only to those officers who clearly needed access to the data for accepted official purposes. Under Doe it would appear that a carefully structured "need to know" system is a constitutional imperative.

Obviously agreement on the desirability or inevitability of a "need to know" system does not answer the question who truly "needs to know" which pieces of data. This article also will not answer that question. The purpose of this article is to develop a logical characterization of medical functions so that a "need to Know" system can be created.

0195-4210/94/$5.00 © 1994 AMIA, Inc.

PRIVACY IN CONSTITUTIONAL LAW

Finding privacy to be a constitutional right does not automatically protect individuals from injury. In the United States, Constitutional rights are essentially "negative" in that they only protect individuals against "governmental" actions. Such rights have no formal effect on non governmental actors. The constitutional right to privacy is therefore necessarily limited to governmental infringement on rights. As with many constitutional rights, balancing of the right of privacy against other legitimate social concerns may be needed.[3] In particular society may demand some compromise to protect public health. Further, a reasonable court might find that few patients would run substantial health risks to protect medical privacy. On the other hand, governments often find it inevitable that they incorporate public constitutional rights into laws regulating private conduct, and state courts might be encouraged to expand the common law right of privacy.

NEED TO KNOW: DEFINITIONS

Developing a "need to know" system requires a sophisticated understanding of medical, social, legal and technological requirements for both privacy and the provision of health care.[1]

Some medical users believe that if data would be useful to a medical professional then that user has a "need to know". Under this thinking a medical researcher has a "need" for any data that might help in research. But in constitutional analysis even a socially desirable activity can only be carried out in a manner which minimizes the intrusion on the protected right. For example, researchers would rarely if ever "need" the patient's identity. As a result privacy protection often requires changes in otherwise convenient methods of administration. It is critical to understand that cost and administrative convenience have rarely been allowed to be balanced against constitutional rights:

"administrative convenience does not justify a policy that otherwise runs afoul of the Constitution"[8]

For example, patient identifiers are often used to simplify administrative tasks. Human names are easily remembered, and may contribute to preventing mistakes in the administration of health care. However, use of names is simply a custom, not a necessity. Distinguishing between those privacy risks which are necessary and those which simply represent administrative convenience is one of the most important tasks in privacy analysis.[2]

For this paper the legal criteria for a "Need to Know" is defined as the **smallest intrusion on the patient's privacy which will permit completion of a well defined socially accepted task.**

NEED TO KNOW: PRIVACY PROTECTION

In the field of computer science, there is a rich literature of methods of implementing privacy protection systems, however it is normally assumed that the job of deciding who should have access to the data has already been done. Few if any medical models of "need to know" have been published, and there is no literature examining the special hazards and opportunities of information systems to create a functional "need to know" system.

A substantial gap exists between the information specialists and the medical community over privacy protection. Information specialists often do not know who needs the information and for what purpose, and the medical community has no idea what privacy protection system might be available. As a result, privacy protection tends to be sacrificed to administrative convenience in the turf battles among the various medical specialties and the administrative and information communities.[2] As networked systems and telemedicine develop and hospitals forge computer links with other health care providers the problems will get worse. Who decides which provider gets access to what data? [5]

The special privacy disclosure hazards of information systems have been widely documented, but information systems also have special privacy protection advantages. Access to data can be controlled dynamically, the data can be easily subdivided and segregated, and real time alerts of security violations can be provided. Basing access to computerized information systems on the historical system of access to paper records both ignores the increased risk of computer systems and the possibility of introducing novel privacy protections. [4]

NEED TO KNOW: DIMENSIONS

Normally data access rights have been structured as "layers", where privileges are greatest on the inside and lowest on the outside. Developments in health care and information systems have rendered such a model obsolete. A consultant, for example, might have a high "need to know", but only for a limited time. Others might have a longer durational "need to know", but only of limited information. Some medical information might be needed by some, but not all clinicians. A pharmacist, for example, rarely needs to know the name of the patient for whom a prescription is being filled. The pharmacist only needs to know that the prescription is authorized, will be delivered to the correct patient and that it does not conflict with other medications for the patient. None of this requires the patient's identity.

"Need to know" should therefore be classified along a series of **DIMENSIONS**. Dimensions are used to categorize the relationship between the data and the person making the request. Dimensions describe the type of patient data, the type of health care provider, the type of data action and so forth. These dimensions can be articulated and classified independently, but interact dynamically. Each dimension affects data access authorization. The core assumption is that each health care worker stands in a definable relationship with each portion of a patient data file.

Using these dimensions computer systems can provide customized "need to know" functionality. Such systems are a product of the examination of the individual institutional health care environment. However a proper dimensional framework assures that key decisions about access are made by policy makers in a deliberate manner. A series of dimensions can be created:

Patient File Dimension

Each patient file is composed of least 5 dimensions:

Identifier information: information which can be used to discover the patient's identity but is not needed for treatment, such as name, birth date, Social security number or universal identifier.

Identifiable information: any information which might be used to generate an identifier, but is otherwise relevant to treatment, such as the date of injury.

Coded identifier: alphanumeric linking tool used to ensure that all data on a patient is linked together. It can be generated for each admission.

Standard medical data: clinically significant medical data which is not "restricted data" as defined below.

Restricted data: data is "restricted" because of its unusual sensitivity and lack of broad medical significance. The classification of restricted data is a social determination and might include categories such as elective abortions, some mental health data, and some pharmaceutical data.

Under either standard or restricted data there might be further subdivisions such as free text or patient codes. Since free text is inherently more capable of creating a security violation, greater access limitations might be justified.

Health Care Worker Dimension

Health care workers are divided by their status in relation to the patient:

Treating team: Health care practitioners directly engaged in regular care of the patient. These would be the people who are routinely allowed to write or execute orders on a patient, and normally have a legitimate knowledge of the patient's identity. The treating team includes several subcategories.

Category 1 members can add members of the treating team and set access. This might be the responsible health care provider.

Category 2 members need general access to patient files. This would include anyone with direct patient responsibility.

Category 3 members need limited access. These are support staff who perform limited functions

Consultants: Health care practitioners who need contact with the patient's data but are not part of the treating team. Consultants usually do not routinely need identifier information or permanent access. Second opinions are treated as a consultation. Usually consultations are addressed to specific individuals, but may be addressed to departments, who then designate the individuals.

Clinical supervision: This category defines the medical authority to review care on specific patients and initiate changes (e.g. clinical quality assurance)

Referral: Authority to transfer a patient to a new treating team, at the same or another institution.

Medical support services (e.g. tests, procedures, pharmacy,transcription): These can be distinguished from consultations when they do not require transmission of the patient file, and are addressed to departments. Support services can use coded identifiers. If identified information is needed, the service is normally a consultation.

File Access Duration Dimension

Duration of access to the patient file is an independent dimension. Even a treating physician may not need access when a patient has left the hospital. Support staff rarely need access when they are not on duty. Some only need access when a specific procedure is being performed. Possible limited dimensions include:

1) access during specific hospitalization, treatment, consultation or referral.

2) timed access (e.g. night coverage)

3) access to archive data only, prevents access to live data on patients currently being treated.

Data File Transaction Dimension

This dimension specifies what transactions are permitted in the file. Some examples include:

Read authority: Authority to read the file

Write authority: Authority to write entries to a file

Copy authority: the right to make copies of a file, for example by down loading to a remote system.

Change authority: authority to determine that an earlier entry should be overruled, either to correct an error or change the record. This is not an edit authority, in medical records all entries must be preserved.

Data Base Authority Dimension

This dimension defines the ability of the user to scan or browse the data base, rather than get information on specific identified patients. Because patient identity can be generated data base authority represents one of the most significant threats to privacy. Users with data base authority can be classified into several groups:

Quality assurance, Cost Control, Long Term Planning and Research: These categories of users review the data base for purposes other than clinical care for a given patient. As just one example these persons might be given access to archived data without identifiers.

Administration, bed control and staff scheduling These and similar tasks require access to current treatment and prognosis data, but not identifiers. An expert system or trusted intermediary might be used to stratify non archived data for immediate administration purposes. Insurance reimbursement can normally use coded identifiers, after an authorization is obtained from the insurer.

System staff: The question of data base access to confidential data by the system staff raises special security problems. However they normally should have no need to know identified data.

Emergency Access Dimension

The system must be arranged to allow temporary emergency access by any health care worker, for example in a typical "code" situation. However the use of emergency access would trigger an immediate quality review, to determine why no authorized user was present and a security review to assure that no security breach was involved.

IMPLEMENTATION

Each institution has to implement the system by examining its own operations and assigning access dimensions. A recent ACM article describes the typical corporate privacy policy as "drift ... until the organization perceived some sort of external threat" and that organizational policies often did not match organizational practice. [12]

Certain principles should govern Need to know systems:

No one should have access based simply on a speculative need under rare circumstances

The emergency override provides an adequate response to any genuine need, and system authorizations can be altered through experience with the system.

Routine access to identifier data should be based solely on the patient's clinical needs.

The key evaluation is whether the patient needs the health care worker to have the identifier data.

Outside access to identified patient data should be strictly limited

Special security precautions are needed before passing data outside the secure system. This means that telemedicine and other extended access to records demands special analysis.[7]

CONCLUSION

The consequences for violating individual's constitutional rights are substantial in both financial and operational terms. System operators can expect detailed scrutiny of their decisions on who gets access to medical data. A "need to know" system appears to be a constitutional requirement. Administrative convenience will not be accepted as a substitute.

Determining who "needs to know" patient information is a special task totally apart from technical "security" analysis. The introduction of information systems initially replicates existing information access environments. However privacy protection often requires confronting traditional methods of operation.

The structure for "need to know" systems proposed here does not attempt to define who "needs to know", rather it defines the appropriate questions which will allow a prototype "need to know" systemto be created. By examining the information flow in a variety of specific environments it is possible to create a wide variety of "need to know" systems suited to the special needs of divergent communities and institutions.

REFERENCES

[1] Brannigan V. "**Computerized Patient Information under the Privacy Act: a Regulatory Effectiveness Analysis**" Pro. 16th Sym. on Com. App. in Med. Care, McGraw Hill 1992: 741-4

[2] Brannigan, V., and R. Dayhoff. **Medical Informatics: The Revolution in Law, Technology and Medicine**, J. of Legal Medicine, Vol 7:1-53.

[3] Brannigan, V., **Patient Privacy, A Consumer Protection Approach**, J. of Med. Sys, 1984, 7:501-505.

[4] Brannigan V. and Beier B. "**Standards for Privacy in Medical information systems: A Technico Legal Revolution**" Proceedings 14th Symp. on Comp. App. in Med. Care, IEEE 1990:266-270

[5] Brannigan V. **Protection of Patient Data in Multi-institutional Medical Computer Networks: Regulatory Effectiveness Analysis** Proc. of the 17th Symp. on Comp. App. in Med. Care, IEEE, Washington D.C. 1993: 59-63

[6] Doe v. New York 15 F.3d 264 (2nd Cir)1/28/94

[7] France FHR Gaunt PN **The need for security- a Clinical View** Int J. Bio Med Comput 35 (Suppl 1) (1994) 189-194

[8] Flores v. Meese 942 F.2d 1352 1991, (US CCA 9th) citing Reed v. Reed, 404 U.S. 71, 76-77, 30 L. Ed. 2d 225, 92 S. Ct. 251 (1971)

[9] Gostin LO, Turek-Brezina J, Powers M, Kozloff R, Faden R Steinauer ED **Privacy and Security of Personal Information in a New Health Care System** JAMA 1993; 270: 2487-2493

[10] H.R. 4077 March 21 1994

[11] Kluge EHW, **Health Information, Privacy Confidentiality and Ethics** Int J. Bio Med Comput35 (Suppl 1) (1994) 23-27

[12] Smith J, **Privacy policies and Practices: Inside the Organizational Maze**, Communications of the ACM Dec. 1993 36: 105-122

[13] Tonks, A **Information Management and Patient Privacy in the NHS**: Brit. Med. J. 307: 6914 P 1227;Nov. 13, 1993

[14] U.S. Congress Office of Technology Assessment: **Protecting Privacy in Computerized Medical Information** Government Printing Office 1993