# Protection of Patient Data in Multi-institutional Medical Computer Networks: Regulatory Effectiveness Analysis

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

*Privacy protection is one of the major issues in the development of multi-institutional clinical information networks. Judicial decisions have confirmed patient's rights to protection of a "reasonable expectation of privacy". Incorporating this protection into a system requires analysis of appropriate models. The National Practitioner Data Bank (NPDB) contains confidential data concerning physician competence. The medical profession had substantial input into the privacy protection features of the NPDB, which are much more comprehensive than those used in many clinical information systems. The NPDB represents the privacy protection which physicians expect for their own data. Regulatory Effectiveness Analysis can be used to analyze the suitability of the NPDB as a model for patient privacy protection. Judicial opinions set public policy and legal structures for privacy, and the NPDB provides an inventory of useable technical tools. After eliminating minor discontinuities, the NPDB can be used as a model to create a useable standard for privacy for multi institutional data transfers.*

## INTRODUCTION

Patient privacy is a major consideration in the development of medical information systems. This paper will evaluate the standards for patient privacy protection in multi-institutional data transfers on wide area networks. For the purpose of this paper a multi-institutional computer network includes any system in which patient data is routinely transferred from one component institution to another for clinical purposes. A "network" includes any system which allows electronic data transfer, including telephone access and electronic mail. It is assumed that "routine data transfer" would be the transmission of the computer-based patient record from one institution to another to (1) provide data to a new caregiver, (2) obtain medical consultations, or (3) obtain insurance or other approvals for treatment. Demand for such systems can be anticipated to increase with managed care or other new approaches to health care cost containment. This paper does not apply to situations involving routine updating of the primary record, or other interactions with the record. This paper is limited to privacy issues: the accuracy of data will be addressed in future work.

Hospitals and physicians cannot automatically assume that compliance with existing single institutional clinical system requirements or the privacy accorded to manual records in inter-institutional transfers sets the level of privacy required in a large computer system. Access to networked systems increases the number of users, the anonymity of the users, the possibility of multiple copies of records and the number of patient records in the system. **Arguably, the risk of invasion of privacy increases exponentially with an increasing number of participants.**

Medical privacy regulations normally do not contain specific technical requirements for computer systems.[1,2,3] Many existing privacy protection systems rely on a kind of "paper" privacy, such as requiring all employees to sign agreements that they will not reveal medical data on patients. This "responsibility" approach does not meet the legal standard for privacy protection. Courts instead look to the actual level of privacy, not forms signed by employees.

## CASES ON MEDICAL PRIVACY

### Whalen

Whalen v. Roe is the leading Supreme Court

0195-4210/92/$5.00 

decision on medical privacy. [4] The computer system in WHALEN was a centralized record of patients who were lawfully prescribed certain drugs which also had unlawful uses. In WHALEN the Supreme Court noted that employees were prohibited from releasing data. However, the court did not consider this prohibition, standing alone, to be sufficient. Before permitting the data bank to operate, the Supreme Court closely scrutinized the protection accorded the data and the small number of individuals who had access to the data:

> The computer tapes containing the prescription data are kept in a locked cabinet. When the tapes are used, the computer is run "off-line," which means that no terminal outside of the computer room can read or record any information. ... At the time of trial there were 17 Department of Health employees with access to the files; in addition, there were 24 investigators with authority to investigate cases of over dispensing which might be identified by the computer.

Finally the Court noted that the data had to be purged after five years. The Court considered the combination of precautions to be critical to the legal acceptability of the system. The WHALEN case is the touchstone for any analysis of medical computer privacy. Any system which does not provide WHALEN protection cannot be assumed to pass constitutional standards. WHALEN protection can be defined as:

1) off line data analysis
2) secure facilities
3) limited data object life
4) limited number of authorized viewers
5) limited purposes for access

WHALEN protection is difficult or impossible to achieve in wide area networks with routine updating of files. However, the bulk transfer of Computer based patient records is easier to analyze and protect.

**Westinghouse**

Networks present new privacy problems but the right of privacy is not static. In all technological developments, courts try to balance new technology with the citizen's "reasonable expectation of privacy". Defining this expectation requires analysis of a number of factors. In Westinghouse [5] the federal court of appeals set out specific factors to be used by a court in weighing privacy rights in medical records:

> The type of record requested,
> The information it does or might contain,
> The potential for harm in any subsequent nonconsensual disclosure,
> The injury from disclosure to the relationship in which the record was generated,
> The adequacy of safeguards to prevent unauthorized disclosure,
> The degree of need for access, and whether there is an express statutory mandate, articulated public policy, or other recognizable public interest militating toward access.

**Behringer**

William Behringer was a physician whose HIV status was disclosed by inadequate hospital protection of the data in his hospital chart. He sued the hospital for invasion of privacy. The BEHRINGER opinion sets a high standard for hospital protection of patient data:

> According to stated policy, charts were limited to those persons having patient care responsibility, but in practical terms, the charts were available to any doctor, nurse or other hospital personnel...the Medical Center had no policy physically restricting access to the HIV test results or the charts containing the results to those involved with the particular patient's care.
>
> the easy accessibility to the charts and the lack of any meaningful Medical Center policy or procedure to limit access that causes the breach to occur. Where the impact of such accessibility is so clearly foreseeable, it is incumbent on the Medical Center, as the custodian of the charts, to take such reasonable measures as are necessary to insure that confidentiality. Failure to take such steps is negligence....
>
> Insuring confidentiality even by Medical Center employees required more, in the present case, than simply instructing employees that medical records are confidential. The charts are kept under the control of the Medical Center with full

> knowledge of the accessibility of such charts to virtually all Medical Center personnel whether authorized or not. [6]

The holding of BEHRINGER is that "paper" protection of privacy is insufficient. Real protection must be built into any system. Adequate regulation of privacy protection may be a formal prerequisite for deciding whether multi institutional systems can be implemented.

What should be the reasonable expectation of privacy in medical data? Many current information systems operate under comparatively loose privacy protection. [7] However, analysis of current hospital systems says nothing about the patient's expectation of privacy, since patients have little or no input into the privacy provided. The most useful approach is to determine what level of protection is provided in a medical environment where the data subjects are in a position to demand their "reasonable expectations of privacy". The next step is to use that level to define the legal standard of a reasonable expectation of privacy for all patients.

## NATIONAL PRACTITIONER DATA BANK

The National Practitioner Data Bank (NPDB) is a large computer system located in Camarillo, California. It is operated by the UNISYS corporation as a contractor to the Public Health Service. The NPDB is a product of the HEALTH CARE QUALITY IMPROVEMENT ACT of 1986. Congress granted antitrust immunity for medical practitioners engaged in "peer review" activities, but mandated the creation of a national reporting system for medical practitioners who had been disciplined, successfully sued for malpractice, or whose hospital privileges had been curtailed. Hospitals, medical societies, malpractice insurance companies and state licensing boards are required to report data to the NPDB. Hospitals are required to get reports from the NPDB when granting privileges to physicians, and every two years thereafter.

Even though the information put into the data bank is often public or semi public, and there is a clear public interest in collecting the data, the confidentiality of the data was a major concern of organized medicine. Physicians and other practitioners did not want the public to have access to the data. In a compromise the release of the data is extremely restricted. Neither patients, nor malpractice insurance carriers can get access to the data. The AMA still expresses doubts as to whether the precautions taken are adequate.

The NPDB operates by collecting reports on physicians submitted by authorized reporters, consolidating the reports together, and sending the consolidated reports, upon request, to authorized institutions. The NPDB process would be analogous to a single request for a patient's entire computer-based medical record, as opposed to a clinical inquiry on a specific visit. As such, it makes a reasonable technical analogy to the proposed transmission of computer based medical records.

The nature of the data involved, the types of transfers, and the prominent role played by organized medicine in setting the privacy requirements are an excellent rationale for using the data bank as a standard for patients' "reasonable expectations of privacy". The Data Bank was developed to protect patient safety, as well as the integrity of the health care system. Prompt access to the data bank may be life critical, and data subjects feel that the data is highly sensitive, and demand protection. Physicians have defined in this data bank what privacy expectations they have for their own sensitive medically related data, and using this data bank to define the standard of privacy would put protection of patient and physician data on an equal level. As one court said:

> the golden rule... requires that one should do unto others as, in equity and good conscience, he would have them do unto him, if their positions were reversed. [8]

## REGULATORY EFFECTIVENESS ANALYSIS

As noted in prior work, Regulatory Effectiveness Analysis can be used to outline a range of possible policy goals and define which legal structures and technical tools support that policy goal. [2] The BEHRINGER case supports a policy goal of a high, though not absolute protection of privacy. Acceptable privacy risks arise from the inherent needs of medical practice, not the administrative needs of the information handler. All the cases cited make it clear that holding someone responsible for a data release is not sufficient, actual protection of the data is required.

The legal structure which fits the public policy requirement is therefore PRECAUTIONS, rather than RESPONSIBILITY.[2] A precautions structure requires specific technical tools. The NPDB model can be examined to determine whether there are discontinuities between the technical tools and the legal structure.

**Technical Data Protection Tools in the NPDB**

To ensure the confidentiality of the data, the PHS took a series of precautions. [9] The computer is physically on the premises of a secure defense contractor, and the system is run in a off line configuration. All persons with access to the computer system must have security clearances. Requests for information can be made electronically, through the same secure COMPUSERVE/INFOPLEX system used by the Internal Revenue Service. This is a high security electronic mail system, where the system managers cannot get access to the data. The requester deposits the inquiry in a mailbox, where it is retrieved by the system computer. No direct electronic connection to the data bank computer is permitted. Requests can only be made electronically from authorized users, who have been furnished with special software provided by the data bank. Although the inquiries are not encrypted, the packet switching system is considered protected against interception.

All requests must be made in a format specified by the data bank, and requests can only be made for a report under the name of the data subject, with appropriate identifying information. No searching of the data bank is permitted. All requests for information are logged, and the log is made available to the practitioner. A copy of any adverse report sent to the data bank is sent to the practitioner. Provisions for disputing the report are available to the physician. No telephone inquiries are allowed, and requests from practitioners for their own records must be notarized. All reports are sent by mail. No electronic responses are currently permitted, although such responses are being explored. The author was advised that any reply would be encrypted, and sent only to the e-mail address of the entity which made the inquiry.

The data bank is wholly self supporting, with an access charge of $6 per hospital inquiry. More than a million inquiries were made in the most recent year. Persons reporting data, and physicians requesting copies of their own files are not charged. The entire privacy system is enforced by civil penalties of up to $10,000 per violation, which can be collected by the HHS inspector general.

**Discontinuities**

Three discontinuities in the NPDB are apparent. First while each inquiry must be made by an authorized entity, there is no requirement that the individual practitioner authorize the inquiry. The second discontinuity is that there is no technical tool to control the purpose for which data is requested, although the applicable regulation appears to limit the lawful purposes for getting the data. These discontinuities appear to be an administrative oversight, not a deliberate decision. The problem exists because the applicable regulation says that a health care entity may request a report from the data bank if they "may be entering employment or affiliation relationships" with the practitioner. This language would be broad enough for a hospital to obtain data on any practitioner in the community, without their consent or advance knowledge. Of course the practitioner would have knowledge later if a personal request was filed, since the other request would appear on the log.

The third discontinuity is that there is no limitation on how long the inquiring hospital may keep the information. Once the data has been received from the NPDB, the only restriction is that it not be disclosed. There is obviously a risk of stale data, but that relates more to accuracy that confidentiality. The indiscriminate retention of records poses a real risk of disclosure that may not be counterbalanced by a need for the data. Unless there is a demonstrated need for a permanent record, either the data could be purged, or the data object itself could be programmed to self destruct after a period of time, unless consent for a permanent record had been granted. None of these problems is especially difficult. Consent forms, need to know certification and data purging can be required to obtain access, without substantial change in the data bank operation.

## DATA PROTECTION STANDARDS

Using BEHRINGER and WHALEN to set public

policy and legal structures and using the NPDB as a source for technical tools permits definition of a "reasonable expectation of privacy" for patient records. After correcting the discontinuities noted above, the NPDB appears to provide a reference standard for the technical requirements for a reasonably secure multi-institutional system for transfer of patient records. Even in its present form such a system would have the following capabilities:

- **Restriction to authorized requesters by a requirement of possession of the restricted requesting software**
- **Password protection to identify individual requesters**
- **All requests come through a secure e-mail system, no direct electronic connection to the data bank**
- **Data search only by patient name, no random browsing of the data bank**
- **Audit trail available to the data subject**
- **Secure data facility, separate from the treating institution**
- **Responses sent in a secure manner, only to pre approved addresses**
- **Possibility of disputing incorrect or unneeded data**

The system could easily have the following additional capabilities:

- **Electronic responses, sent encrypted through secure e-mail to a mailbox accessible only to user with authorized decryption software. (under study)**
- **Search only for an authorized purpose (possible)**
- **Search only with request of patient (possible)**

## CONCLUSION

Proper concern for patient privacy is not merely a design criteria for multi institutional clinical networks. The concern for privacy may determine whether such networks are created at all. Paper protection of privacy will not be acceptable to courts and prompt and technologically sophisticated responses to privacy concerns will be necessary to establish wide area networks. The computer system used for the National Practitioner Data Bank provides a model for protecting patient privacy in bulk transfer of records on multi institutional wide area networks. With simple upgrades, such a system would provide a substantial level of privacy protection for transfers of computer based patient records.

## References


1.Brannigan, V. 1984 **Patient Privacy, A Consumer Protection Approach**, J. of Med. Systems 7:500-505.

2. 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

3. Brannigan V. and B. Beier. 1991 **"Standards for Privacy in Medical information systems: A Technico Legal Revolution"** Proceedings 14th Sym on Com App in Med. Care, IEEE:266-270

4 Whalen v. Roe 429 U.S. 589; 97 S.Ct. 869; 51 L. Ed.2d 64 February 22, 1977

5. United States of America v. Westinghouse Electric 638 F.2d 570 3rd Cir (1980)

6. Estate of William Behringer M.D. v. The Medical Center at Princeton, 249 N.J. Super. 597; 592 A.2d 1251; April 25, 1991

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

8. Nowell v. Great Atlantic & Pacific Tea Co., 250 N.C. 575, 108 S.E.2d 889, 891 (1959)

9. Dept. of Health and Human Services **National Practitioner Data Bank Guidebook: A Reference for Individuals reporting to and Querying the Data Bank (with 1992 Supplement)**



Author's thanks to Dr. Rene Koslow, Dr. Ruth Dayhoff and the Public Health Service