COMPUTERIZED PATIENT INFORMATION UNDER THE PRIVACY ACT: A REGULATORY EFFECTIVENESS ANALYSIS

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

ABSTRACT

Regulatory Effectiveness Analysis is a new technique for measuring compliance with a technological regulatory system. By examining the public policies, legal structures and technical tools involved in the regulatory system, it is possible to discover discontinuities which may result in non compliance with the regulatory system. This technique can be used to analyze the Veterans Health Administration's (VHA) actions under the Privacy Act.

INTRODUCTION

This article is designed to apply a new legal technique to the regulation of patient privacy in government hospitals. The Privacy Act is the major federal protection of individual privacy for data contained in systems of records maintained by the federal government. (1,2,3) The VHA has installed a sophisticated hospital information system at most of its locations, and the regulatory documents for the VA hospitals are available for study.

REGULATORY EFFECTIVENESS ANALYSIS

Regulatory effectiveness analysis (REA) is a method for evaluating the success of an existing or proposed regulatory program. It is under development at the University of Maryland. REA is designed to measure separately and together three key components of a technical regulatory system.

The first component is the set of **PUBLIC POLICIES**. Public policy is a narrative statement of the goals to be achieved by the regulatory program. These statements can be either concrete or abstract.

The second component is the set of **LEGAL STRUCTURES** used to implement the regulation. Regulation requires a legal mechanism to enforce the social will on individuals who would not otherwise comply.

The third component is the set of **TECHNICAL TOOLS** available for regulation. Every technology has a distinct and often limited set of technical tools available. Technical tools are not limited to machines or laboratories. Encryption, ID cards, IQ tests, statistical quality assurance and double entry bookkeeping are all technical tools.

The theory of regulatory effectiveness analysis is that all three of these components must be properly designed to achieve a working regulatory system. Public policies must be coherent; legal structures must contain all necessary elements; and technical tools must be available and produce the needed results. Further, the components interact. Public policy, legal structures and technical tools have interlocking sets of requirements and capabilities. **REQUIREMENTS** are the preconditions which must be satisfied by other components before a given component can function. **CAPABILITIES** reflect the ability of a tool to satisfy a requirement of another component.

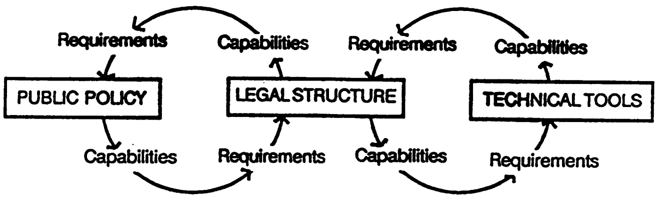

Figure 1 Regulatory effectiveness analysis

Figure 1 shows the interaction of the three components and their respective capabilities and requirements. For example, each specific public policy requires certain capabilities in the legal structure. Similarly, each legal structure has capabilities that can satisfy the needs of public policy.

Regulatory effectiveness analysis is a study of 1) whether the components of a system are clearly defined and 2) whether the capabilities and requirements of a given set of components are properly matched. If a component is ill defined or there is a mismatch between policy goals, structure and tools a **DISCONTINUITY** exists. For example the Food and Drug Administration was supposed to regulate software under the 1976 Medical Device Amendments. The legal structures established under the 1976 amendments were premarket approval or product standards. However, both of these legal structures require a technical tool which can test a given piece of software and determine how safe it is. Such a tool did not exist. This created a discontinuity, which required changing be described as a legal structure where the policy maker has determined in advance which technical tools must be implemented and the individual has the obligation of carrying out the specific acts. Under the precaution approach the individual is supposed to implement the tool, but is not expected to determine whether the tool will perform the intended function satisfactorily. For the PRECAUTION structure to function:

a) a defined individual must carry out the action
b) the action to be carried out must be specified
c) a method for determining the action has been carried out must be specified.

In the RESPONSIBILITY structure a defined person is assigned the obligation to prevent an injury from occurring with potential penalties if they do not. For the RESPONSIBILITY structure to function it requires:

a) a defined individual who will be sanctioned for the default,
b) the default, the injury and the sanction must all occur in a reasonably short time
c) the sanction must be sufficient to deter the unwanted conduct
d) the responsible individual must have actual control over the default
e) the injury must be traceable to the defined default.

The two structures have different requirements and possibilities. Under **responsibility** the person has discretion to choose the methods of avoiding the injury. The sanction is imposed for failure to choose an adequate method. Under the **precaution** approach, the discretion has been exercised by the individual who defined the precaution.

Technical Tools

The regulatory effectiveness analysis has two questions:

1) Do legal structures exist which properly implement the technical tools?
2) Do the legal structures and technical tools acting together correspond to the policy statements contained in the Privacy Act?

There are two technical tools noted in the DVA Federal Register notice: "need to know" and passwords. It is necessary to determine which legal structures have been chosen to implement the technical tools. The implementation of the required security procedures is governed by the 1991 draft MANUAL for VA Computer Operations.(12) For example the manual states:

there shall be no local modification of the .... security software features...codes shall be changed at least once every 90 days...all ...user access shall be through the kernel security system

Despite these individual instances of PRECAUTIONS, it is clear from reading the manual that the VA is relying primarily on the RESPONSIBILITY tool for staff compliance with the act. Numerous passages assign responsibility. However, as noted above there are specific criteria for a functioning responsibility system. The first criteria is a defined individual who will be sanctioned. However, responsibility in the VA is not clearly defined.

The manual describes in detail the Medical Information Security Service (MISS), however, that office is not given authority to review and approve security precautions for local facilities, but only authority to:

assists with office and facility management of information security activities as requested

At the local level the manual also indicates conflicting duties:

The Facility ISO (information security officer) is... responsible for management and coordination of an information security program...

but:

the health care facility chief, IRM service or system manager shall be responsible for implementing security procedures at their facility.

and :

VHA facility management shall ensure that appropriate data security features ... are utilized

Even at this early stage a problem is obvious. Exactly **who** is the person responsible for developing and implementing the security program? And what are they responsible for doing? If the legal structure is responsibility, the system is already showing signs of discontinuity.

Even more serious, there is no definition whatever for one of the key technical tools, the "need-to-know" system. The Federal Register notice states that the VA actually controls access to data on a need to know basis. However, the entire implementation of the need to know concept is indicated by a single line in the manual:

16.08 (a) Use of VHA information assets... is restricted to those with a need for them in the performance of their duties.

The operations manual defines no standards or requirements for the need-to-know system, and identifies no individual who is to ensure that one exists. It is unclear why the VA, which felt it necessary to specify how long a password must be, does not feel it necessary to establish a "need-to-know" policy and enforce it on local facilities, or even establish a requirement for a local policy.

Agency Responsibility versus Local Control

The Privacy Act makes it an agency responsibility to determine: "**the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records**". The Federal Register notice states that the VA has made the policy decisions and set out requirements for the systems. However, the actual security policy appears to be determined by the local facility manager, not the agency. With very few exceptions, there are no limitations on their freedom of action.

> **Each VHA facility is responsible for designating the sensitivity of the data/information under its administrative control**

In particular, the Federal Register notice does not disclose that the medical system is accessible from remote locations, although it discloses that other systems are accessible. However, the manual states:

> **16.10 b (1) Remote off-site (e.g. Dial in) access to the computer system may be authorized locally.**

Therefore not only is the Federal Register notice misleading, but the VA officials signing the Federal register notice are not determining the security policy.

Policy on Information Security Risks

Local officials are given very broad discretion to decide how great a security risk they will take:

> **16.14 Budget constraints, staffing limitations, cost benefit considerations ....may result in the acceptance of certain risks**

As a result the only mandated security precautions are reflected in the password requirements. However, as has been shown in other research, and acknowledged in the manuals, any password based system is vulnerable if remote access is permitted to the system.(13) Telephone lines are easily monitored, and passwords can then be used for access to the system. The manual shows an understanding of the risk of interception of transmitted data:

> **16.07 b (6) Transmission of data, text and images. Depending on the sensitivity of the material, different protective measures may be used such as line protection devices of(sic) encryption/ decryption procedures**

Even within a facility passwords have limited value in establishing responsibility. Passwords are not self authenticating, are easily copied, and may be discovered randomly. The VA is aware of the security risks to the system, but does not control what risks the system managers take. The only required audit is every two or five years. As a part of these audits the Security program assessment and the Risk analysis are to contain the critical information about what is the actual level of privacy risk contained in the system.

> **Vulnerabilities found during any analysis shall be corrected or accepted as uncontrolled risks by the facility director**

In other words, under this provision there is no absolute responsibility to protect privacy, but only a responsibility to document once every two or five years, in a confidential report, what the facility feels is the acceptable level of risk! While the Director of MISS is informed of the risk being taken at the local level, there does not seem to be any authority to change the local decision. Interestingly, unlike patient data, the risk analysis and security assessment are handled under required security precautions:

> **16.13.d Personnel performing a external risk assessment shall consider the assessment written results as a sensitive document, results should be viewed on a need to know basis. A copy of the report shall be sent, using the double envelope method, to the director, MISS....The Riso shall keep one copy in a secure file.**

The Manual requires certification of Privacy Act Compliance for all new applications and significant modifications to existing systems. However, it does not require that the agency official making the certification be provided with the risk analysis documenting the uncorrected vulnerabilities in the system! The certifying official is provided only with a summary report.

Personal Computers

The FR notice also requires that personal computers meet the same level of security:

> **Information that is downloaded ...and maintained on personal computers is afforded similar storage and access protections as the data that is maintained in the original files.**

There is simply nothing in the manual which provides a legal structure or technical tool to carry out this policy.

RESULTS

Regulatory effectiveness analysis has uncovered a number of discontinuities.

1) The policy stated in the Privacy Act is precaution oriented, however, the legal structure adopted by the VA is responsibility oriented. However, the responsibility is diffused among several different places and the audit system does not "close the loop".

2) The actual security system is under the jurisdiction

of local officials who are authorized to make the decision that a certain privacy risk is acceptable, but the information on that decision will be kept somewhat more confidential than the patient data itself.

3) The statute requires a statement of the safeguards in the system. The Federal Register notice promises a need to know system. However, the Operations Manual does not define a "need-to-know" system.

4) The Federal Register notice does not disclose that local officials have the right to both allow remote access, and determine what level of security is used on those remote connections.

5) There are no technical tools or legal structures to guarantee that the downloaded information on personal computers is actually afforded the level of protection stated in the Federal Register notice.

6) The individual who certifies compliance with the appropriate rules and statutes may not be sent the actual security data on the systems.

7) The key discontinuity is that the VA does not have in place a centralized regulatory structure which sets standards which local facilities must meet.

CONCLUSION

Regulatory effectiveness analysis appears to be an effective means of pinpointing discontinuities within a regulatory compliance program. However, it should not be assumed that a discontinuity indicates a failure of will in complying with a statute. As the FDA example shows, avoiding discontinuity may require adjustment of the policy goals, as well as refinement of the technical tools.

As a result, nothing in this article should be taken as a special criticism of the Department of Veterans Affairs. They make available the documentation needed to do the regulatory effectiveness analysis. Other agencies have not even attempted to conform to the requirements of the act. Also, it is not clear that there exists any workable combination of tools, structures and policies which would afford patients the privacy contemplated by the Privacy Act. The open nature of hospitals, the life critical nature of access to data, the huge number of employees and the need for 24 hour access make the technical job extremely difficult. Third, nothing in this article describes the actual level of patient privacy protection in the VA. Actions which are not mandated by regulation will not be captured by this type of analysis. The closing date for documents used in this article was December 1991. Any changes made in the draft manual after that date will not be reflected in this paper.

REFERENCES

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

2) Brannigan V. and Beier B. **Standards for Privacy in Medical information systems: A Technico Legal Revolution** Datenshutz and Datensicherung 1991 Vol 9 pp 467-472

3) Brannigan V. and Beier B. **"Standards for Privacy in Medical information systems: A Technico Legal Revolution"** Proceedings 14th Symposium on Computer Applications in Medical Care, IEEE 1990:266-270

4) Brannigan, V., **The Regulation of Medical Software as a Device Under The Food, Drug and Cosmetic Act,** Jurimetrics J. of Law, Sci. and Tech, 27: 370-382.

5) Brannigan, V., **The Regulation of Medical Computer Software as a Device Under The Food, Drug and Cosmetic Act,** 10th Sym. Comp. App.in Med Care,IEEE 1986:347-354

6) Brannigan V. **"Software Quality Regulation under the Safe Medical Devices Act of 1990: Hospitals are now the Canary in the Software Mine"** Proceedings 15th Symp. on Comp. App. in Med. Care Mc Graw-Hill 1991:238-242

7) THE PRIVACY ACT 5 USC 552a

8) Beier, B. and Brannigan V., **Principles for Patient Privacy Protection: USA and Germany,** MEDINFO 83 Proc. Fourth World Conf. on Med. Inf. Van Bemmel, Ball, and Wigertz, Amsterdam, 1983, 967-970.

9)Brannigan, V., **Patient Privacy: A Consumer Protection Approach,** Proc. of the 7th Symp. on Comp. App. in Medical Care, IEEE, 1983: 648-651

10) 56 FR 1054

11) Brannigan, V., **Defining Consumer Science, A Legal Scholar's View,** Proceedings of the National Inv. Conference on Consumer Science in Institutions of Higher Education, July 5-9, 1982, Madison, WI.

12) D. of Veterans Affairs INFORMATION RESOURCES MANAGEMENT MANUAL (7/30 1991)

13) Brannigan, V., **Remote Telephone Access: The Critical Issue in Patient Privacy Protection,** Proc. of the Eighth Symposium on Computer Applications in Medical Care, IEEE, Washington D.C. 1984: 575-578.