

DEPARTMENT OF HEALTH & HUMAN SERVICES

Public Health Service

Substance Abuse and Mental Health Services Administration

Rockville MD 20857

**CONFIDENTIALITY
AND
THE APPROPRIATE USES OF DATA**

Prepared by

**Alan L. Ziglin, Ph.D.
Consultant
5300 Cedar Chase
Dunwoody, GA 30338**

for

**The Nebraska Department of Public Institutions
through funding from the U.S. Center for Mental Health Services**

May, 1995

TABLE OF CONTENTS

	PAGE
INTRODUCTION.....	1
BACKGROUND.....	1
CONTEXT.....	2
THE DELICATE BALANCE: DATA FOR DECISION MAKING VERSUS THE PROTECTION OF CLIENT RIGHTS.....	3
VALUE AND NEED FOR DATA.....	3
Clinical and services management issues.....	3
Administrative issues.....	3
Evaluation, assessment and research Issues.....	5
The most important need for data.....	5
NEED FOR PROTECTION.....	6
APPROPRIATE AND INAPPROPRIATE USES OF DATA.....	7
RECOMMENDATIONS: ASSURING THE BALANCE.....	8
COMPUTER SECURITY.....	8
TRAINING.....	10
LEGISLATION/REGULATION.....	11
PUBLIC INFORMATION.....	12
POLICIES AND PROCEDURES.....	13
DATA STORAGE AND SECURITY.....	14
INFORMED CONSENT.....	15
PLANNING.....	15
LOCUS OF RESPONSIBILITY AND STRUCTURE.....	16
REFERENCES.....	17
ACKNOWLEDGMENTS.....	20
APPENDICES	
APPENDIX A - LITERATURE REVIEW	
APPENDIX B - METHODOLOGY	
APPENDIX C - ILLUSTRATIVE EXAMPLES OF ETHICAL ISSUES	
APPENDIX D - DRAFT MODEL LEGISLATION	
APPENDIX E - ISSUES OF INFORMED CONSENT	

INTRODUCTION

BACKGROUND

The field of mental health and mental health public policy is replete with myth, rumor and fad. Often it is discovered that today's mental health public policy or administrative agenda is the result of yesterday's inaccurate impressions or assumptions about persons with mental disorder and their utilization of services. Accurate data, appropriately utilized, is the best defense in ensuring that mental health public policy, administrative, and clinical decisions are grounded in the reality of those persons who need mental health services and accurately reflect the ways in which they are, or are not, served by the mental health system. Therefore, accurate and reliable information becomes a critical tool for public policy and an important counter to many of the myths and misconception that surround persons with mental disorder and their treatment.

However, the need for these data does not mitigate the fact that the data are sensitive. There have historically been, and continue to be, important concerns about confidentiality and appropriate uses of these data. That is, the basis of the data is personal, individual information which, if used inappropriately, could have negative consequences for the very individuals the service delivery system is supposed to *be helping*. We are reminded of this fact every time the news media reports an incident in which they indicate that the alleged perpetrator was a "former mental patient".

The topic of confidentiality and appropriate uses of data in the mental health service delivery Systems has been an issue for over three decades. The Literature Review found in Appendix A contains citations of many articles and books which well documented this. Among some of the more salient are Kupfer, et al. (1976), Laska and Banks (1975), Westin (1976) and the report on the Conference on User-Oriented Mental Health Information Systems (1975). Attention has been called to the topic at various times by clients/consumers, family members, clinicians, and administrators held accountable for the service delivery system. The topic always relates, either directly or indirectly, to the possibilities realized by the proliferation of computers and automation. The dilemma traditionally has surrounded the fact that while administrators need data in order to make administrative decisions; enhance the quality of services; and to justify resources needed by the service system, the data are sensitive.

In light of this, and concerns raised by some of Nebraska's Regional Program Administrators and community-based mental health service providers, the Nebraska Department of Public Institutions requested technical assistance from the National Institute of Mental Health (now the Center for Mental Health Services). While confidentiality is a broad area, this project was to focus only on confidentiality as it related to automated data systems. The request made was that a project be funded to look more comprehensively at this topic. The result was to be a set of guidelines which any organization or agency could utilize in addressing this complex set of interrelated issues. This document summarizes the process and the resultant recommendations regarding guidelines, which

derived from the Technical Assistance activity. The methodology utilized is outlined in Appendix B.

CONTEXT

In today's world of managed care, data are used more and more in ways they have never been used before, such as for decisionmaking on resource allocations at the individual level. The context within which we must consider the issues of confidentiality, appropriate uses of data, and protection of those data, has clearly changed. Data are being shared among organizations, which increases the risk of problems with misrouting, mishandling, misinterpreting, and generally, misusing these client-sensitive and potentially stigmatizing data.

One implication of the context in which data are used, revolves around the ethical dilemma of pitting the confidentiality rights of an individual against the rights of others. Illustrative examples of such ethical issues are provided in Appendix C. The problem involves weighing the right to privacy of one individual against the need of another person to be protected.

A second contextual issue involves the sharing (and potential subsequent sharing) of data. With each episode of sharing, the possibility of a breach of confidentiality, or misuse of data increases. The risk of sharing data becomes an even more critical issues, in light of the inevitable changes in the healthcare system. Whether the future relies heavily on Managed Care or some other system, more complicated and sensitive data will need to be collected. Given the need for quality improvement programs, and the potential of report cards, providers reporting to networks, networks reporting to health plans, health plans reporting to alliances, and alliances reporting to states, there is an increased danger of violations of confidentiality and/or inappropriate uses of data.

Among the many aspects of the issue of protection is the question of who should have access to the data. Ethical issues are raised regarding the collection, storage, transmission (electronic or physical), utilization and subsequent dissemination of the data. Ethical issues are especially relevant today because of a significant societal shift which has taken place. As Donaldson and Lohr (1994) point Out (p. 210), historically the ethical issues involved the benefit to the individual as opposed to the risk to the individual. However, increasingly now the ethical issues involve the benefit to organizations and society as opposed to the risk to the individual. illustrative examples of these types of ethical issues are also presented in Appendix C.

Beyond the traditional aspects regarding the need for protection of data, more recently there has been a realization that the data are needed by more than just administrators. Clients, family members, clinicians and others are also becoming reliant on the data. In this environment, the potential negative consequences of misuse of the data becomes even greater.

The third type of contextual issues deals with the dangers of routine handling of confidential data. Due to the sensitivity of the data being collected, the importance of

protection is obvious. However, clinicians and staff work with sensitive data so routinely that it is easy for them to inadvertently become lax about protection of the data. Beyond this point, Otto et al. (1991) found mental health professionals to be, "...poorly informed about the nature and extent of confidentiality..." With the stigma which unfortunately still surrounds mental illness, even the information that a person has received services needs to be protected. However, sometimes the right to privacy is overshadowed by the "need to know" of others. For example, should the right to privacy of the individual be protected if the life or safety of another individual is threatened? Obviously, a balance needs to be maintained between the right to privacy of an individual and the "need to know" of others.

THE DELICATE BALANCE: DATA FOR DECISION MAKING VERSUS THE PROTECTION OF CLIENT RIGHTS

The discussion in this section will focus on a brief review of the value of, and need for, data. This review will lead into considerations necessary in protecting the data and the privacy of individuals. The final area to be discussed regarding establishing and maintaining this "delicate balance" will center around the appropriate and inappropriate uses of the data.

VALUE AND NEED FOR DATA

A project recently completed (Ziglin, 1993) for the Center for Mental Health Services (formerly the National Institute of Mental Health) stressed that the need for data in the public sector mental health service delivery system was oriented around: clinical and services management issues; administrative issues; and evaluation, assessment and research issues.

Clinical and services management issues

Prime among legitimate needs for data are clinical and services management issues such as: available services (both within and across agencies), assessment and promotion of continuity of care, and service planning. Proper utilization of data promotes quality services and a client focused system. It allows service providers to be aware of what approaches (clinical and otherwise) have been most successful with which types of clients in terms of diagnosis, treatment goals, and where the consumer currently is in his or her recovery process.

In addition, data form the basis for such critical components of a responsive clinical environment as: case management, utilization review, and quality improvement/performance measurement. All of these activities are oriented around assuring that the services represent a good value to the consumer.

Administrative issues

Administrative needs require data for planning, administrative and programmatic

decisionmaking, resource allocation, accountability, and policy development. Obviously, the major administrative need for data is accountability. This need is heightened by the reality that public sector services are funded through a diverse set of funding streams. This requires the ability of the service system to be accountable for the system as a whole, and not simply for how individual funds are expended (Ziglin, 1991).

Accountability also takes on a new depth of meaning when one considers the range of constituents to whom the service system is accountable. In addition to the historically traditional accountability to funding sources and elected officials, the public sector service delivery system in the 1990's also finds itself accountable to clients, family members, staff, and others. While this broadened vision of constituents certainly promotes an openness and quality focus which is bound to benefit clients, it also calls for a robustness of data which makes the availability of data additionally important. Indeed, some who have historically been skeptical of data collection activities, now find themselves among the primary users of these data.

There is a significant need for data for many purposes. Leginski, et al. (1989) state that ("p.8), "a primary stimulus to providing better Systems to care for the mentally ill is decisionmaking by managers to make informed and rational changes. Data describing the operation of their organization are a critical input to these decisionmakers.... Decisions can.. be made about both the resources and actions thought necessary to effect... system changes."

A recent book edited by Grasso and Epstein (1993) reinforces these points repeatedly. In one case (p.92) they refer to a program where outcomes were improved based on decisions which were made after analyzing available data. In another case (p.122) there is a discussion of a program where desired outcomes, as articulated by a program, were found to be counterproductive and were subsequently changed after a full examination of the data.

Another critical need for data is in the area of planning and resource allocation. It is critical that there is a solid understanding, not only of the needs of persons with mental disorder but how those needs are being met, or are not being met, by the system. Such knowledge allows for better planning for future services and for more effective and strategic allocation of scarce resources to maximize the ability of the system to meet the needs of persons with mental disorders.

Another important value of data is to deal with rumor and myth both within organizations and in response to the news media. Sensational press coverage or charges by public officials can greatly damage public and political support for mental health services. Valid and reliable data can be appropriately used to diffuse and refute inaccurate, but sensational, charges by the news media and public officials.

Also, within organizations, rumors and myths develop that can deter effective care and/or demand administrative action that would be counterproductive to the overall mission of the organization. An example of one such situation took place at a state mental hospital where the clinical staff was demanding that the administration refuse all referrals from the

Department of Corrections because the clinical staff believed that the Department of Corrections was abusing state hospital resources as a way to simply extend an inmate's incarceration. However, through examination of data over the prior two years it was discovered that there was only one case, albeit a sensational one, that really supported those concerns. Abrupt administrative action cutting off referrals from the Department of Corrections would have caused unnecessary interagency conflict and political repercussions, but also would have denied appropriate treatment to a number of persons.

It is apparent that many different sectors of our society must work together collaboratively to be fully responsive to the needs of persons with mental disorder. Accurate and reliable data become critical in facilitating interagency collaboration and collaboration between public and private sectors.

Evaluation, assessment and research issues

In the area of evaluation, assessment and research, a primary focus is on performance monitoring and improvement. Future changes in our healthcare system will likely mandate data for evaluation and assessment purposes. As the revision of our healthcare system evolves, it will become clear that, at its heart is the need to evaluate the effectiveness and appropriateness of various providers and treatment types, for various types of consumers and constituencies.

In addition, one potential use of data is for research other than evaluative research. What is meant by "other than evaluative research" is research for the purpose of furthering scientific knowledge. Obviously, research related to public policy and management is a legitimate use for information systems. On the other hand, research uses for expanding scientific knowledge would not justify ongoing data collection activities. However, when data are already collected for the purposes outlined above, a substantial ancillary benefit accrues from knowledge gained through non-valuative research activities.

An example of such benefit is found in the research work of E. Fuller Torrey, Ann E. Bowler and Robert Rawlings (Kurstak, 1991). For well over a century, there has been speculation that influenza might be related to the occurrence of psychosis. Torrey and his associates wanted to explore a specific aspect of this possibility. They wanted to investigate whether the exposure of a woman to influenza while she was pregnant would cause her baby to be more likely to develop psychoses in adulthood. Such a research study would have taken generations to investigate prospectively. However, given the existence of over a decade of client data from existing public sector mental health service delivery system databases, the researchers were able to investigate their theory. The fact that they did not find a relationship between perinatal influenza infections and subsequent schizophrenia-prone births was important in advancing scientific knowledge about brain diseases.

The most important need for data

As important as the data needs for clinical and services management, administrative issues, and evaluation may be, there is an over-arching need which crosses all three areas

and which deserves to be highlighted separately. That topic is the more recently underscored need for data to enable and empower consumers as they make healthcare choices. Given the seriousness with which the public sector mental health service delivery system views consumer empowerment, a primary need for data must be to serve as a foundation for that empowerment. While consumers of mental health services and their family members have historically been among the most skeptical about the need for data, they now find themselves among the primary users of these data. As Campbell and Frey (1993) point out, people are interested in using data for such purposes as:

- deciding where to seek medical and hospital care;
- making healthcare system decisions; and
- making treatment choices.

Buckley (1993) discusses uses of technology in order to assist consumers in making healthcare choices. She also stresses the importance of data regarding available service resources, cost, and effectiveness in allowing consumers to make informed choices about the services that will support their recovery.

Given that there is a substantial need for the data, the next issue which arises is the issue of protection.

NEED FOR PROTECTION

The issue is no longer whether or not data should be collected, or whether data should be stored electronically. These are givens in the current behavioral healthcare environment. Since there are important and justifiable reasons to collect data, the issue now becomes how to best protect the confidentiality of the data and the privacy of the persons about whom (and from whom) the data were collected. Along with this issue comes the topic of how to ensure that safeguards are in place to enhance the likelihood that data will be used appropriately.

Given the number and complexity of issues involved, many previous efforts have been focused on certain specific issues while ignoring, or attending only superficially, to others. Due to the sensitivity of the data being collected, the importance of a comprehensive perspective on protection issues is obvious.

As has already been stressed, there is significant potential harm if information provided about (or from) a recipient of mental health services is used inappropriately. This is likely to be the case as long as there continues to be a stigma associated with Mental Illness. The potential harm is not limited to recipients of service. Harm is also a potential issue for family members and service providers. In addition, there is potential harm from inaccurate or inappropriate data provided to legislators or other constituents.

Another type of harm occurs if misuse of data causes a person to be less likely to seek needed services, or to be less likely to encourage a family member or friend to seek needed services. If the credibility of the service delivery system and its providers is

diminished, all persons involved are harmed, in some way.

While the issues above are important, one significant issue of harm bears separate consideration. At the center of the issue of harm is the need to distinguish appropriate and inappropriate uses of data. The members of the Task Force which provided input into this project had substantial comments in many areas, but one of the areas of greatest interest was that of distinguishing appropriate and inappropriate uses of data. This concern was far broader than expressing a need to establish a list of appropriate uses. Some of their concerns centered around the integrity of the data system itself. If pertinent and accurate outputs are created, those providing the data will be increasingly motivated to assure the quality of the data being submitted. However, poor quality data can lead to poor quality administrative decisions with resultant negative implications for quality of services.

APPROPRIATE AND INAPPROPRIATE USES OF DATA

As has already been noted, there is potential harm from inappropriate uses of data. This topic will also be addressed in the Recommendations Section. However, it bears underscoring.

An exhaustive discussion of appropriate and inappropriate uses of statistics and statistical data is beyond the scope of this project. However, the agency collecting and distributing the data has an obligation to assure that data they share with others is not misleading. They are also obligated to display data in an understandable manner. Further, there is a responsibility to minimize the risk of subsequent inappropriate uses of the data by providing adequate footnotes and caveats to assist the recipient and user of the data. This often requires that the agency releasing data have some understanding of what the requestor is attempting to determine. One issue here is determining how "raw" or analyzed the data should be when released. Just because the requestor may not be knowledgeable enough to articulate the question correctly, does not mean that the agency should simply blindly respond to the request. There may be relevant intervening variables, or the time period of data requested may not be long enough to realistically establish a trend. For example, hospital admissions are higher at certain times of the year. If a requestor of data were unaware of this and requested admission data for a month that had an unusually high number of admissions, they might extrapolate a grossly inaccurate picture of what annual admissions were. Another example would be if someone interested in hospital overcrowding requested admission and discharge data. It would be important for them to understand that there were many other variables relevant to hospital overcrowding, a few of which are: average length of stay, diagnostic categories, and outcome indicators.

Outputs need to make clear any limitations of the data, such as the fact that the database may reflect only publicly funded programs. In addition, outputs need to be focused on decision support, not only for administrators, but for specific constituent groups. That is, for example, outputs intended for consumers or others who do not work for the service delivery system should not use abbreviations or terms which will make the data difficult to interpret and use

Particular attention is needed when data are being used comparatively. If providers or programs are to be compared it is important that the setting, services, types of clients, funding, etc. are sufficiently similar so that the comparison is reasonable.

Protection means not only protecting data, it also means assuring the appropriate use of those data. Any data or information is a potentially powerful tool. However, when the data refer to a topic which is surrounded by stigma, it is additionally important to assure their appropriate application.

RECOMMENDATIONS: ASSURING THE BALANCE

The topic of confidentiality is the nexus for many interrelated issues. There is, of course, the issue of physical security of data. This requires attention being given to computer security and policies and procedures being articulated. Once security, and other procedures are in place, there is a need to train all appropriate persons. In addition to underscoring the importance of confidentiality, part of that training needs to stress the sanctions for violating the procedures. At the same time it is important that a public information initiative assures that all stakeholders are aware of the emphasis being placed on confidentiality. Public information also serves to establish what expectations the stakeholders should reasonably have of the system.

What is needed is not a series of fragmented, one time solutions, but rather, a comprehensive and ongoing strategy to deal with confidentiality and the appropriate use of data. The strategy should address, at a minimum, the areas discussed below.

COMPUTER SECURITY

The purpose of computer security is to limit access in an effort to protect people, as opposed to systems. An integral foundation for this security is the creation of a corporate mentality (or culture) which instills in all persons involved with the data a sense of personal responsibility for protecting the data. How to create and maintain this corporate mentality will be addressed in the training recommendations. However, a prerequisite for creating a corporate mentality is articulating who has access to the data and for what purposes.

Donaldson and Lohr (1994) provide an excellent list of protective safeguards which include p. 153):

- hardware (e.g., memory protect);
- software (e.g., audit trails, log-on procedures);
- personnel control (e.g., badges or other mechanisms to control entry or limit movement);
- physical object control (e.g., logging and cataloging of magnetic tapes and floppy disks, destruction of paper containing person-identifiable printouts);
- disaster preparedness (e.g., sprinklers, tape vaults in case of fire, flood, or bomb);
- procedures (e.g., granting access to systems, assigning passwords);

-administration (e.g., auditing events, disaster preparedness, security officer); and
-management oversight (e.g., periodic review of safeguards, unexpected inspections, policy guidance).'

Additionally, Webman (1994) raises the potential of data encryption.

It is clear from the above that while no security system is perfect, both software and hardware security need to be put in place such that violation of the system is unlikely, difficult, time consuming, and preferably will leave an audit trail showing that security has been breached. While, hopefully, a breach of security will not occur and the audit trail will not be needed, if needed, it might provide important information on what information was accessed and how.

Software safeguards should include user identification codes which not only allow a user access to the system, but also limit the activities of any given user. For example, access authorization should distinguish those users who can only access data from those who can enter or modify data. There needs to be a sensitivity to who needs access to which data. For example, clinical decision makers need access to data which administrators do not.

Hardware or physical safeguards should include physical (metal key) locking of the hardware, locking of the rooms within which the hardware is located and creating and securing appropriate backup for the system. Policies need to specify who is authorized to be in the area where equipment is located which can enter, access, or modify data.

In addition to presenting a comprehensive overview to computer security, Kochanski (1989) also cautions against too much security, as do Stephenson (1989) and von Matuschka (1992). A careful assessment needs to be made of how much security is needed and useful. The danger is that needless amounts of security are not only costly (in implementation as well as staff costs), but can also lead to less security. That is, if security procedures are too cumbersome, overworked staff may seek expedient shortcuts which intentionally or unintentionally could seriously compromise security.

Procedures for electronically sharing data need to be created not only to protect confidential data, but also to minimize the chances of spreading computer viruses (Greenberg, 1989).

Data encryption (Dror, 1989 and Webman, 1994) also promotes security by storing data in a coded format. In addition, other techniques for securing data should be investigated. Prime among them should be consideration of the feasibility of storing individual client data separately from the client identifying information. Thus, client name, social security number, etc. could be stored in a file separate from all the other data on the client. Each file could have a common identifier. This would allow the files to be linked when necessary, but otherwise, violation of one file would limit the information available.

Finally, in securing a system, it is important to remember that all security risks are not external (Juris, 1986). Disgruntled or poorly trained staff, internal to the system, can also

present threats to security.

TRAINING

Training is a critical aspect of confidentiality and appropriate uses of data. Confidentiality training has been specifically suggested to be legislatively mandated by one group involved with proposed Health Care Reform training (Webman, 1994). Training in the area of confidentiality needs to begin with the creation of what might be called a "corporate mentality". That is, if one were to poll employees in an organization and ask who is responsible for protecting the confidentiality of client data, the response would often be the name of a specific person or a specific group of persons. However, the appropriate answer is, "Everyone"!

As Davenport (1994) points Out, with regard to building cultures, "...technologies alone won't change anyone's behavior." Training to develop a corporate mentality is critical in helping all persons involved with the service delivery system to understand that everyone has a shared responsibility when it comes to confidentiality. The training can be accomplished in multiple ways. A few examples are: sub-state training, training trainers, and contracting for training.

Beyond this, training should be ongoing and should focus everyone on the applicability of established guidelines, policies, and laws. Training is the responsibility of all organizations involved with the collection and use of the data. In some instances this responsibility should be articulated contractually. Among topics to be addressed would be:

- why confidentiality is important;
- what constitutes confidential data;
- who can access which data and for what purposes;
- issues of transmission and misrouting of information;
- issues of redisclosure; and
- informed consent.

As mentioned above, training is a continual process. Its ongoing nature is important, not only to share new information, but to reinforce previously discussed topics. Training needs to be simple and "down to earth". To a clerical staff person with what seems like eighty hours of work to do in forty, it may seem quite reasonable to post the access code to the computer system on the wall above the terminal. This way it is always available for quick access. However, the training process would hopefully help the clerk understand that this would undermine security, even if the trainer does not mention this specific scenario. The training is part of the process of helping everyone involved with the system to understand that they play an integral part in protecting and assuring confidentiality.

Since a major goal of the training activities is to build a corporate mentality, one idea would be to not assign the training responsibilities to those in the organization who are usually responsible for training. Rather, a group of interested staff with varying work duties and professional training could take responsibility for creating the training. This would help keep

the training from becoming too "academic TM. ~ this manner, when the training is presented, those being trained would be aware that the impetus and perspective of the training was from those with jobs and responsibilities similar to their own. At the end of each training session participants could be polled for ideas, not only on how to improve future training, but also for ideas on how to promote the creation of the "culture" ~osters, suggestion box, etc.).

While the purpose of the training should not be to frighten the trainees, the training should be clear in its portrayal of both legal and ethical issues. Role playing activities might be helpful.

LEGISLATION/REGULATION

There is a dual purpose to be served by creating legislation and regulations regarding confidentiality and appropriate uses of data. First, the existence of such legislation would serve to additionally sensitize all persons involved to the seriousness of the issue. It would underscore that protection of confidentiality was far more than a well-intentioned action. Secondly, legislation would provide clear sanctions for those who violate confidentiality.

Healthcare information is very personal and sensitive information protected by our constitutional right to privacy. If this information is improperly used or released, it may seriously harm the ability of a client to obtain employment, education, insurance, credit, and other necessities. Therefore, as electronic information management Systems are developed the potential for improper computer access to healthcare files (computer crime) must be considered. Computer crime has significantly increased in recent years and the development of computer crime statutes has lagged behind. Therefore, there is a need for sanctions to punish breaches of confidentiality. These sanctions should be based in legislation and reiterated in contracts, as well as, policies and procedures.

The sanctions need to be enforceable and need to distinguish accidental from deliberate violations. In addition, the legislation needs to address mandated reporting issues such as reportable diseases.

Donaldson and Lohr (1994) cite (pp. 181-182) efforts of the Workgroup on Electronic Data Interchange. They suggest a legislative emphasis on, "... computer system security, fair information practices, and privacy protection."

They suggest that legislation should:

- establish uniform requirements for preservation of confidentiality and privacy rights in electronic health care claims processing and payment;

- apply these requirements to the collection, storage, handling, and transmission of individually identifiable health care data, including initial and subsequent disclosure in electronic transactions by all public and private payers, providers of health care, and all other entities involved in the transactions;

- exempt state public reporting laws;
- delineate protocols for secure electronic storage and transmission of health care data:
- specify fair information practices that ensure a proper balance between required disclosures, use of data, and patient privacy;
- require publication of the existence of health care data banks;
- establish appropriate protections for highly sensitive data, such as data concerning mental health, substance abuse, and communicable and genetic diseases;
- encourage use of alternative dispute resolution mechanisms where appropriate;
- establish that compliance with the act's requirements would be a defense to legal actions based on charges of improper disclosure;
- impose penalties for violations of the act, including civil damages, equitable remedies, and attorneys' fees where appropriate; and
- provide for enforcement by government officials and private, aggrieved parties.'

Model legislation language, developed by the American Health Information Management Association, is included in Appendix D. It is included to illustrate the types of issues and penalties (both civil and criminal) which might be relevant in drafting legislation.

PUBLIC INFORMATION

Through public information initiatives, the constituents of the service delivery system can be made aware of the priority the organization places on confidentiality. Among specific topics are:

- that an information system exists;
- potential benefits to the public of the information system; the expectations which are being established regarding confidentiality;
- what safeguards and sanctions are in place;
- how to bring concerns to the attention of the appropriate persons;
- what constitutes informed consent;
- how consumers can review and correct data; and
- how the organization assures protection of client rights.

Since public information is the external counterpart of staff training, as part of their corporate mentality-building activities, the training group could also be involved with public information. Besides content, consideration needs to be given to how to "get the message out". Some of the possibilities include posters at service delivery sites, pamphlets, and

public service announcements in the news media.

The primary target of such efforts should be the many diverse constituents of the system (service recipients, family members, staff, legislators, the public at large, etc.).

POLICIES AND PROCEDURES

The recommendations regarding Policies and Procedures really "cut across" all areas of recommendations. Any given recommendation may require a policy with which to enforce it. In this section the discussion will focus on specific areas where policies and procedures were identified as needed during the course of this technical assistance activity. Some topics will need to be addressed differently based on whether individual or aggregate data are at issue, or whether individual or organizational accountability are being addressed.

What constitutes a breach of confidentiality needs to be defined and measures taken to diminish the chances of such breaches occurring. DeKraai and Sales (Kratochwill and Morris, 1991) define breach of confidentiality as the "...voluntary disclosures or the threat that someone who has legitimate access to confidential information will wrongfully disclose that information." They go on to discuss exceptions such as reporting abuse or dangerous persons. Breaches can be intentional as well as accidental, and could be electronic or otherwise. Among other ways, breaches can occur by word of mouth, printed material, computer transferred material, or information sent by facsimile machines.

According to one recent article, (Gostin, et al.,1993) technological " . . . advances in electronic systems are proceeding at an accelerated pace. Data protection policies, if they are to be effective in this rapidly changing environment, must not be tied to specific systems and system capabilities but rather, must establish security protection guidelines that define system goals but do not specify how these goals will be reached." Gilbert (1993) lists five examples of policy topics for healthcare providers as: "general policies as to the management and use of the patient records," "staff training," "patient information," "physical security measures," and "protection of software, hardware and telecommunication tools". Among specific areas and topics to consider for inclusion in policies and procedures are:

- clear roles and responsibilities for protecting data;
- the need for a single point of data entry preferably close to the original source of the data);
- mechanisms for, and issues to be considered in, transferring data;
- authority for various types of database access (individual, aggregate, organizational);
- requirement of an audit trail and specification of who is responsible for monitoring its existence and use;
- safeguards surrounding electronic dissemination of information;
- provision for all contracts to specify and fix responsibility regarding access to, and distribution of, data;
- specification of standardized procedures for secure storage of data and disposal

- of output documents;
- accidental electronic and physical misrouting of data;
- procedures for reporting, and responding to, breaches; and
- defining appropriate ways to respond to individual data requests (for example: how, and under what circumstances, information can be shared with law enforcement agencies).

The agency has a responsibility to ensure that its data are used appropriately. For this reason, there is a need for policies regarding appropriate uses of data. These policies need to first focus on assuring that appropriate data are used for a given purpose. Secondly, policies need to:

- reinforce the importance of appropriately analyzing data;
- placing data within an appropriate context (turning data into information); and
- using adequate caveats and qualifiers to promote appropriate uses of the data.

In addition, how the data (both aggregate and individual) will be used needs to be specified. In this area, it is important to specify when redisclosure of data would be appropriate and whether interagency data linkages are acceptable.

Policies also need to be clear regarding how clients can access and review data about themselves. A part of this policy needs to articulate how a client can challenge and/or change data about themselves. In a given situation, it may not be possible for data to be changed, and if this occurs, there needs to be a mechanism to note that the client disagrees with that information.

DATA STORAGE AND SECURITY

Most attention given to data storage and security focuses on data currently being actively used. However, it is recommended that specific attention be given to long term issues. Intensive security can transition to lax security when data become archived.

A related issue deals with determining when data lose their meaningfulness, or stated another way, how long data should be kept. While there is no widely accepted guideline, the determination needs to be based on clinical issues. That is, after what period of time is it not relevant that a person has received services. In a study conducted almost twenty years ago (Noll and Hanlon, 1976), mental health state office directors were asked how long they kept client data. One fourth of the replies indicated six months to ten years, with the median response being four years. However, over half (57%) indicated data were kept indefinitely.

Realistically, the fact that a person was seen briefly for an evaluation seventeen years ago and not served since then, is not likely to be useful data. Thus, on a clinical basis a timeframe (perhaps five years after the person last received services) needs to be set. After that length of time has elapsed since the person last received services, the data are either destroyed or client identifying data (name, address, social security number, etc.) are

stripped from the record and destroyed. This would leave the rest of the data (nonclient identifiable) available for nonclinical aggregate data uses.

INFORMED CONSENT

Protection issues revolve around who and what are being protected. At the heart of this topic is the concept of informed consent. That is, what consents are required and how timely must the consent be? What constitutes informed consent? Are there situations in which informed consent is not possible and, if so, what is the appropriate procedure? Efforts need to be made to assure that the person providing the consent has an understanding of relevant issues.

Donaldson and Lohr (1994) indicate consent must ~. 203):

- be in writing or electronically provided in an acceptable manner;
- be signed or authorized electronically by the individual on a date specified;
- be clear about the entities being authorized to disclose information;
- be specific about the nature of the information to be disclosed;
- be specific as to the institutions or persons to whom the information may be disclosed;
- be specific about the purpose for which the information may be used, both at the time of the intended disclosure and at any future time; and
- be specific as to the date when the authorization expires."

If the issues are not understood by the client, the consent is not "informed". Donaldson and Lohr (1994) also stress ~. 150) that if the data content are not known by the client, the consent cannot be informed.

Quinlan, et al. (1993) have presented materials relevant to the topic of informed consent. These materials are attached in Appendix E.

PLANNING

The assuring of confidentiality and the appropriate use of data must be an ongoing process. The recommendations of this document should serve to assist the mental health authority in promoting this important function while pursuing its mission. However, given the issues and concerns previously enumerated, it becomes clear that this is a complex area filled with issues which overlap with each other. It would be all too easy to simply say, "See that everyone in the system does what is right, and see to it that there are substantial sanctions if they do not comply!." However, determining what is "right" is often neither easy nor obvious. Therefore, in addition to laws and policies/procedures, guidelines become extremely critical. Further, as technologies and social issues/sensitivities evolve, the "ground rules" must also be adjusted.

The point here is that what is needed in dealing with confidentiality and appropriate uses

of data is a process rather than a product. What is needed is not an immutable list of things which must, or must not, be done; rather, what is needed is a process to assist in formulating the laws, policies/procedures, and guidelines initially and then keeping them current and viable as technology and issues evolve.

A comprehensive strategy speaks to the issue that the variety of recommendations addressed in this document need to be set forth in a coordinated and integrated way such that they provide a comprehensive approach to confidentiality and appropriate use of data. The specific aspects of computer security, policies and procedures, training, etc., must not only be integrated and coordinated with each other, but also fit well within the overall structure and work of the agency. The systems that are set in place to ensure confidentiality and appropriate use of data cannot be such that they work at cross purposes or present barriers to the overall organizational efficiency. If they do, they are likely to be ineffective. Therefore, what the agency needs to do is develop a plan for ensuring confidentiality and appropriate uses of data. Among other functions the plan will need to address, it will be important to assure ongoing review to include:

- periodic review of what data should be collected and how long data should be retained;
- periodic review of procedures;
- oversight on intra- and inter-agency sharing, and uses, of data;
- addressing issues of data transmission, both physical and electronic;
- issues surrounding use of unique client identifiers; and
- independent investigation of alleged misuses of data or violations of confidentiality.

It will also be imperative that persons involved in this process keep current with changes in many relevant areas including: technology; legal issues; legislation; healthcare reform; compliance audits; best practices and quality improvement. As Gostin, et al. (1993) stated, the "...steps identified by the National Research Council as necessary for achieving greater computer security and trustworthiness include quality control, access control on program code as well as data, user identification and authorization, protection of executable code, security logging, a security administrator, data encryption, operational support tools to assist in verifying the security state of the system, independent audits of the system, and hazard analysis. Levels of access can also be established recognizing the varying degrees of security required for differing kinds of information."

LOCUS OF RESPONSIBILITY AND STRUCTURE

It will be necessary to clearly establish a Locus of Responsibility and Structure in order to assure the success of this process. Such a mechanism could be a special advisory group or a coordination of some ongoing input by existing advisory groups or boards. Regardless, it is imperative that substantive input be made by a diverse set of stakeholders including clients, advocates, family members, local providers, state level staff, researchers, and other interested persons.

This Locus of Responsibility and Structure will need to assign responsibility for the

implementation of the plan. It will also be necessary to assure that adequate authority and resources are available in order to implement the plan. Secondly, it will be important to set up some mechanism whereby the development of the plan, its implementation, and the ongoing operation of what it puts in place, is fully informed by a variety of perspectives and can be modified to meet new and changing demands in the environment.

REFERENCES

- Buckley, Susan M. Moving MHSIP Toward a Person-Centered Paradigm. Unpublished concept paper submitted to the Federal Center for Mental Health Services and the Mental Health Statistics Improvement Program Ad Hoc Advisory Group, August, 1993.
- Campbell, Jean, PhD, and Elizabeth Doore Frey Humanizing Decision Support Systems. Unpublished document. Maine Department of Mental Health and Mental Retardation, 1993.
- Conference on User-Oriented Mental Health Information Systems: A Renort. [NIMH. ADM-42-74-90(OP)] Atlanta, GA:Southern Regional Education Board, April, 1975.
- Davenport, Thomas H. Saving IT's Soul: Human-Centered Information Management. Harvard Business Review 119-131, March-April, 1994.
- Donaldson, Molla S. and Kathleen N. Lohr, editors Health Data in the Information Age: Use, Disclosure, and Privacy. Washington, D.C. National Academy Press, 1994.
- Dror, Asael Secret Codes. Byte 267-270, June, 1989.
- Gilbert, Francoise, Esq. Telemedicine Issues Using Computer and Telecommunication Technology in the Delivery of Healthcare: Legal Aspects. Department of Health and Human Services, Office of Rural Health Policy Rural Telemedicine Workshop, November 3-5, 1993. Copyright 1993.
- Gostin, Lawrence O., JD, Joan Turek-Brezina, PhD, Madison Powell, JD, PhD, Rene Kozloff, PhD, Ruth Faden, PhD, Dennis D. Steinauer Privacy and Security of Personal Information in a New Health Care System. Journal of the American Medical Association 270(20):2487-2492, 1993.
- Grasso, Anthony J. and Irwin Epstein, editors. Information Systems in Child, Youth, and Family Agencies: Planning, Implementation, and Service Enhancement. New York:The Haworth Press, 1993.
- Greenberg, Ross M. Know Thy Viral Enemy. Byte 275-280, June, 1989.
- Gulbinat, Walter. Balancing Individual and Societal Needs: Micro- vs. Macro-Ethics. Behavioral Healthcare Tomorrow 3341, January/February 1994.

Hargrove, David S. Ethical Issues in Rural Mental Health Practice. Professional Psychology: Research and Practice 17(10):20-23, 1986.

Health Information Model Legislation Language. American Health Information Management Association, February, 1993.

Juris, Robbin Keeping Out the Insiders. Computer Decisions 18:4849, 1986.

Kochanski, Martin How Safe Is It? Byte 257, June, 1989.

Kratochwill, Thomas and Richard J. Morris, editors. The Practice of Child Therapy. Massachusetts:Allyn, Inc., 1991.

Kupfer, David J., Michael Levine, and John A. Nelson. Mental Health Information Systems: Design and Implementation. New York:Marcel Dekker, Inc., 1976.

Kurstak, Edouard, editor. Psychiatry and Biological Factors. New York:Plenum Medical Book Company, 1991.

Laska, Eugene M. and Rheta Bank, editors. Safeguarding Psychiatric Privacy: Computer Systems and Their Uses. New York:John Wiley and Sons, 1975.

Leginski, Walter, A. PhD, and Colette Croze, John Driggers, Shirley Dumpman, Dennis Geertsen, PhD,

Edna Kamis-Gould, PhD, M. Jo Namerow, PhD, Robert E. Patton, Nancy Z. Wilson, and Cecil Wurster.

Data Standards for Mental Health Decision Support Systems. NIMH Series FN No.10. DHHS Pub. No.

(ADM)89-1589. Washington, D.C. U.S. Government Printing Office, 1989

Noll, John O., PhD and Mark J. Hanlon, MA Patient Privacy and Confidentiality at Mental Health Centers. American Journal of Psychiatry 133(11): 1286-1289, 1976.

Otto, Randy K., James R. P. Ogloff, and Mark A. Small Confidentiality and Informed Consent in Psychotherapy: Clinicians' Knowledge and Practices in Florida and Nebraska. Forensic Reports 4:379-389, 1991.

Quinlan, James L., Amy S. Bones and John M. Ryan Confidentiality of Medical Records and Consent to Treatment. Unpublished material presented at conference sponsored by the Division of Community Health Nursing of the Nebraska Department of Health, and Development Systems, Inc., Region VII Title X Training Office, June 10, 1993.

Stephenson, Peter Personal and Private. Byte 285-288, June, 1989.

von Matuschka, Heinz Graf How Much Computer Security? Across the Board 29:12-13, 1992.

Webman, Dorothy, MSW Provider Recommendations for Safeguarding Patient Confidentiality. Behavioral Healthcare Tomorrow 33-37, January/February 1994.

Westin, Alan F. Computers. Health Records. and Citizen Rights. National Bureau of Standards Monograph No.157. Washington, D.C. U.S. Government Printing Office, 1976.

Ziglin, Alan L., PhD Reporting Requirements and MHSIP: The Appropriate Relationship Between Accountability and Data Standards for Decision Support Systems. Unpublished document prepared for the National Institute of Mental Health. August, 1991.

Ziglin, Alan L., PhD The Importance of Unique Client Identifiers in the Public Sector Mental Health Service Delivery System. Unpublished document prepared for the Federal Center for Mental Health Services. November, 1993.

ACKNOWLEDGEMENTS

Ultimately, the success of a project of this nature relies heavily on the Task Force members. Each of the members of this Task Force provided invaluable insights and expertise. Task Force members included:

Robert Bussard, MPA
Program Specialist
Division on Alcoholism and Drug Abuse
Nebraska Department of Public Institutions

Gina Dunning, JD
Legal Counsel
Health and Human Services Committee
Nebraska State Legislature

Eric Evans
Deputy Director
Nebraska Advocacy Services

Gail Flanery, PhD
Deputy Director
Voices for Children in Nebraska
Omaha, Nebraska

George Hanigan, MA
Director
Community Mental Health Center of Lancaster County
Lincoln, Nebraska

James Harvey, CMSW
Quality Improvement Coordinator
Office of Community Mental Health
Nebraska Department of Public Institutions

Christine McCollister
Quality Assurance Manager
Lincoln/Lancaster Drug Project
Lincoln, Nebraska

Suzanne Ortega, PhD
Professor
Department of Sociology
University of Nebraska-Lincoln

M. Thomas Perkins, PhD, ACSW

Regional Program Administrator
Scottsbluff, Nebraska

Dan Powers, JD
Consumer Liaison
Office of Community Mental Health
Nebraska Department of Public Institutions

Thomas Safranek, MD
State Medical Epidemiologist
Nebraska Department of Health

Dan Ullinan, PhD
Senior Clinical Psychologist
Lincoln Regional Center
Lincoln, Nebraska

Larry Weniger
Director
Information Management Services
Nebraska Department of Public Institutions

Task Force Staff:

Peter G. Beeson, PhD
Director of Planning
Nebraska Department of Public Institutions

Mark DeKraai, JD, PhD
Youth Mental Health Administrator
Nebraska Department of Public Institutions

Paula Hartig
Planning/Information Specialist
Office of Planning
Nebraska Department of Public Institutions

Michelle Larson, JD, MA
Student Intern
Office of Planning
Nebraska Department of Public Institutions

In addition to the role played by the Task Force members, the Federal Center for Mental Health Services (CMHS) provided not only financial support for this project, but also access to Ronald W. Manderscheid, Ph.D. whose contributions are greatly appreciated.

Particular appreciation is expressed to Ms. Michelle Larson for her assistance in locating reference materials, to Ms. Paula Hartig whose efforts were invaluable during the latter stages of this project, and to Dr. Peter Beeson who, as Project Director, remained a driving force throughout this project.

To all the above, the project consultant, as author of this document, expresses sincere appreciation.

APPENDIX A

LITERATURE REVIEW

SAFEGUARDING CLIENT PRIVACY AND DATA CONFIDENTIALITY

IN MENTAL HEALTH INFORMATION SYSTEMS:

A REVIEW OF LITERATURE

Alan L. Ziglin, Ph.D.

March, 1993

INTRODUCTION

This report is a concise review of relevant literature dealing with citizen rights and the use of computerized information systems in the field of mental health. The report was guided by five main issues that arise while designing and implementing mental health information systems. They are: 1) the need for collecting client data and their accrued benefits; 2) client loss of privacy and the need for confidentiality of collected data; 3) processes to reduce the concerns of clients regarding privacy and confidentiality; and 4) model policies and procedures that are available to safeguard confidential information in health information systems. Some of the legal measures proposed by authors under the third issue, at times overlap with discussions of model policies.

A two pronged approach was adopted while collecting relevant literature. Journal articles were limited to U.S. publications from 1985 to the present (a few exceptions were made to include some seminal contributions), while books and monographs from 1975 forward were included in the report. The 1975 date was chosen in order to include a collection of very significant publications from the mid-1970's through the early 1980's which dealt, in a comprehensive manner, with the issues of computerized health records and the rights of clients.

The databases that were accessed to search for literature include Medline, PsycLit, SocioFile, InfoTrac, the Social Science Index, and the on-line library indices of Georgia State University, Emory University and Georgia Institute of Technology.

I. The Need For And Benefit Of Automated Client Data

With greater public acceptance of psychiatric treatment, there are more demands placed on the mental health service delivery system. The rising demands lead to the need for better management and accountability of mental health programs (Kupfer et al., 1976; Ziglin, 1991). Initially authors describe three areas where data are needed. According to Laska and Bank (1975), as well as Leginski, et al. (1989), client data can be used for administration and decision making functions, for program evaluation and for clinical management. They also describe how client data can be used to analyze clinical information, demographic information, information about resource utilization (staff, physical, financial) and help in planning and evaluation. Zawadski and Gee (1984) emphasize the need for maintaining client data in information systems to meet various federal guidelines and state regulations that require health programs to report cost, services provided and relevant census data. Computerized health information systems also help manage hospital operations more efficiently, monitor staff service activity, improve customer service and help plan programs for particular client groups. These functions are very important in times when funding for social programs are limited. The use of information systems to better manage facilities, and provide more efficient and improved quality of service is discussed in detail by a number of authors (Snyder, 1986; Bennett and Trute, 1983; Bank, 1981; Binner, 1988; Alexander et al, 1985; Sherman, 1987; DeTore, 1988; Zieserl, 1989; Robinson, 1990; Baskin and Seiffer, 1990).

While most of the above mentioned authors specify the administrative need for maintaining

client data and the benefits that result, the need for data in order to conduct productive research is stressed by others. Till and DeBoer (1983), discuss the use of mental health information systems to foster research and increased collaboration between practitioners and researchers. Client data are also essential to conduct epidemiological research and gain a better understanding of external factors related to mental health issues (Bank, 1981). Computerized record keeping also vastly increases research capacity and provides for considerable cost advantages (Trute, Tefft and Scuse, 1985; Romano, 1987).

More recently various clinical applications of mental health information Systems have been proposed in a series of articles Baskin, 1990; Mezzich and Mezzich, 1990; Plutchik and Karasu, 1990; Greist, 1990). Computerized data information systems can significantly impact automated psychiatric testing, computerized clinical interviewing, client diagnosis, emergency treatments and other methods of clinical decision making (Hedlund, 1987,1988; Schwartz, 1984; Schwartz, 1990). Authors like Blouin et al.,1988 and Greist, 1988 also forcefully suggest the need for more research into the clinical applications of mental health information Systems.

Apart from influencing administrative and clinical functions, medical information systems also affect auxiliary professions and departments like nursing and the pharmacy. According to Aydin (1989), the introduction of an information system increased interdependence between departments in a medical center and led to greater communication, cooperation and ultimately better working relations between the departments. Nurses and other clinical personnel also used information systems more frequently and as a result, improved their productivity (Campbell et al., 1989).

Finally information systems are essential to keep up with the demands for information and make use of the advancements in technology (Hogan and Essock, 1991; Dowling, 1989). McDonald (1989), predicts more efficient use of medical data and increased cost-cutting through advances in medical information technology such as hand held computers, CD-ROM storage and retrievals, computerized home monitoring and diagnosis, etc. A health care reform bill has also been introduced by U.S. Representative Nancy Johnson, which would mandate that all hospital medical records be computerized by 2001 and a nationwide network of computerized patient records be created (Larkin, 1991).

While most authors emphasize the various benefits of a mental health information system, it would be difficult to say that the public overwhelmingly support such a system. Very few public opinion polls have been conducted regarding the issue of privacy and computerized mental health records. However, a Harris Poll in 1977 found that when subjects were asked about collecting and storing private mental health records in computers, 48% of the respondents believed the benefits of such a system outweigh the dangers, and 40% believed that the dangers outweigh the benefits (Katz, 1990). Even though this poll is fifteen years old, it strongly suggests that the concerns of the public need to be taken seriously.

II. Issues of Client Privacy And Data Confidentiality

The issues of safeguarding the privacy of clients and maintaining the confidentiality of sensitive data are integral parts of the process of designing and implementing medical information systems. These issues gain even more importance in mental health information systems. Longitudinal studies have shown that concern over privacy and the use of computers rose gradually in the 1970's (Dutton and Meadows, 1987). In the 1980's the level of concern rose more rapidly. According to Katz (1990), in 1983 only 19% of those surveyed were "very concerned" about safeguarding the privacy of information stored in computers, while in 1989 this figure rose to 35%.

Since collection of personal information is widespread in many areas of our society, the central issue of concern is not the collection and maintenance of data, but rather control over who will access the data (Taylor and Davis, 1989). Computers give rise to unique risks to privacy and confidentiality especially with regard to data-banks in shared or multi-user systems (Trute, Tefft and Scuse, 1985). Presently, most medical information systems are accessed by various government agencies and large insurance corporations. Technological advances provide easier access to such data-banks and there is concern that this will increase the power of bureaucracies over the individual and lead to greater surveillance (Gandy, 1989).

Administrative and clinical data are more sensitive to misuse than statistical data (Trute et al., 1985). Dickens (1983) warns readers about political and legal institutions misusing these data and undermining the confidentiality of data in mental health information systems.

Researchers discussing the issues of privacy and confidentiality in medical information systems often enumerate the concepts involved. Ware (1975), provides a list of thirteen different concepts which relate to privacy and computerized medical records. They include: privacy, personal privacy (information/computerized records), invasion of privacy, data privacy, confidentiality, computer security, network security, data security, integrity of data or system, access control, seepage and linkage. Other important sources of definitions are Curran and Bank (1975), Romano (1987), Griesser et al., (1980) and the report of the Conference on User-oriented Mental Health Information Systems (1975).

Though computerized data banks provide the benefits discussed above, their disadvantages are also well recorded. Young (1982), gives a number of specific examples to illustrate problems related to use of inaccurate data, misuse of data and the collection of too much data. Westin (1976), outlines incidents in Michigan, Washington and New York dealing with the impact of computers on citizen rights, especially in mental health organizations. In all three incidents, there was strong opposition to the use of personal identifiers in personal and diagnostic reports stored in computers. They were said to violate the rights to privacy and the medical confidentiality of patients. The various intentional and unintentional breaches of security and the confidentiality of both client information and administrative information are discussed by Schmauss (1991). He describes intentional breaches of security as those caused by computer "hackers" who may steal, damage or intercept data, or unauthorized access by an employee who views, uses, alters, prints or copies data stored in computer files. Unintentional breaches are caused by untrained or

poorly trained employees, and malfunctions in hardware or software systems. Processes to reduce these breaches of security are discussed below. However, the most comprehensive analysis of the various threats to privacy, data integrity and usage integrity is provided by Griesser et al., (1980). General overviews on the subject of computers and privacy in medical information systems can also be obtained from articles by Wolkon (1986) and Scholes (1986).

Finally, Westin (1982) believes that the management of the health care delivery organizations are responsible for protecting citizens rights, and creating organizational policies which keep up with the various uses of computerized data-banks. The importance of the role of management is also emphasized by Bank and Laska (1978), who suggest that the utilitarian potential of computerized information systems can be fully realized only if the clients gain confidence in the ability of the organization to safeguard their privacy and keep information confidential. In addition, Grady and Romano (1991) point out that organizations must be aware that confidentiality cannot be absolute in the rapidly changing world of automated information.

III. Processes To Safeguard Privacy And Maintain Confidentiality

In order to gain the confidence of clients, management can use legal, technical and organizational measures to safeguard privacy and confidentiality, especially in a multi-user mental health information system bank and Laska, 1978; Laska et al., 1975). The technical measures can be further broken down into hardware and software methods (Griesser et al., 1980).

Some of the organizational measures proposed are:

- If information is shared among government agencies, then the agency seeking information maintains standards of confidentiality comparable to the original agency (Pollock, 1991).
- informed consent forms are signed by clients to permit usage of data by other agencies (Schwartz, 1986; Trute et al., 1985).
- Creating a permanent committee on confidentiality to review client privacy (Pp.13. Conference on user oriented MHIS).
- Facilitating client access to data in order to verify and correct (Trute et al., 1985).
- Introducing an agency-wide confidentiality policy (Harvey, 1988).
- Creating a central data protection registrar and instructing all data users to register themselves and comply with some common security principles (Hedlund, 1988).

- Confidentiality training and education for staff responsible for operating and using the information system (Schmauss, 1991).
- Organizing frequent confidentiality awareness campaigns, using various methods such as posters, slogans (Grady and Romano, 1991).

More detailed and comprehensive discussions of organizational measures can be found in, Westin, 1982; Griesser et al., 1980; Bank, 1981; Hedlund, 1988; Schwartz, 1984 and Mednick, 1982.

Some of the technical measures proposed are:

- Using software security methods including "audit trails" to discourage data misuse (Schmauss, 1991).
- Creating "user identification" methods such as passwords, machine-readable badges, and other forms of physical user identification (Schmauss, 1991).
- Eliminating personal client identifiers to prevent breaches of confidentiality (Bennett and Trute, 1983).
- Restricting the transfer of records so that it is not possible to track clients across programs report of Conference on User-Oriented MHIS, 1975).
- Storing sensitive data in either aggregate or de-identified form report of Conference on User-Oriented MHIS, 1975).

Other detailed software and hardware measures of security are discussed by Sauter, 1977; Peterson and Fenna, 1977; Reichertz, 1977; Sidowski et al., 1980; Ting, 1990; and Griesser et al., 1980). Griesser et al. (1980), also systematically explain the various steps involved in selecting appropriate protection measures and those which are cost effective. But the level of technical security measures for information systems is limited only by the funds available for the purpose (Schwartz, 1986). Many authors also note that the most sophisticated and recent methods are found in the field of computer science dealing with information systems and database management (Hoffmann, 1977; Paton and D'huyvetter, 1980).

Some of the legal measures proposed are:

- Changes in the 1974 Privacy Act to empower individuals, make agencies more accountable, and strengthen laws to prevent misuse of data (Regan, 1986).
- Legislation to safeguard various aspects of client rights, help provide organizational security measures and guidelines to maintain usage integrity

(Koch, 1975).

Monographs by Westin (1975), and Griesser et al., (1980) provide some of the best discussions and critiques of the various legal measures available to protect confidentiality and citizen rights. The following discussion on model policies provides more references which address this issue.

IV. Model Policies And Procedures

A number of components of a medical information system need to be taken into consideration in order to provide overall security for confidential data and maintain client privacy. The data to be entered into the system is just one component. Hedlund et al. , (1977) suggest that limits be placed on the amount of data to be collected, as omnibus mental health information systems provide greater risks. Trute et al., (1985), and Knesper et al., (1978), point out the need for extensive discussion before identifying specific data to be included, and reviewing in detail who will ultimately utilize the data.

The macro-level design of the mental health information system also plays an important role in affecting the levels of security (Wurster and Goodman, 1980). The report of the Conference on User-Oriented MHIS (1975) provides a discussion on the advantages and disadvantages of a centralized and decentralized mental health information system and an analysis of nine different factors that affect this choice.

A number of authors analyze the various legal models proposed by various states. Curran and Bank (1975), describe laws pertaining to medical confidentiality, mental health records, privacy law, data-banks and computer services in Connecticut, Hawaii, Massachusetts, New York, Rhode Island, Vermont and the District of Columbia. Nye (1980), also compares and analyzes four federal bills introduced to protect the privacy of medical records, and critiques them in the context of our increasingly computerized society. She applauds the access provisions of 'S503', 'HR3444/S865' and 'HR2979' (two Senate Bills and two House of Representatives Bills) that provide for client access to records, right to correct a record, requirement of written client consent for certain disclosures and limitations on redisclosure. Her criticisms address the provisions set aside in each bill for, "governmental discovery and disclosure of personal information without patient consent, and, under certain circumstances, without patient knowledge (Nye, 1980. p. 653)." She also raises questions about provisions in the bills for the use of medical information by law enforcement authorities. The applicability of federal confidential protection for alcohol and drug abuse client records in safeguarding mental health records is considered by Lanman (1980). Other model legal policies are proposed by the American Medical Association, American Civil Liberties Union, IBM Medical Department, Department of Health, Education and Welfare (HEW), Society for Internal Medicine, and the National Association of Blue Shield Plans (Westin, 1975).

The responses of a comprehensive survey administered to Departments of Mental Health in all the fifty states in 1976 can help identify the basic components of a model policy (Hedlund, 1978). Ninety-nine percent of the respondents said that it was "critical &

essential" that normal hospital regulations with regards to medical records be strictly followed while using computerized records. Sixty-nine percent wanted special hospital regulations to deal with computerized medical records. Sixty-six percent wanted physical security to control access to the computers. Sixty percent wanted special software to control access. The survey also revealed that in 71% of the departments all patient identification information was eliminated. Finally, 80% of the respondents indicated that federal laws help regulate the use of computerized medical information systems.

Discussions on existing mental health information system; also provide data on model policies that help protect client privacy. Kuper, Levine and Nelson (1976), give detailed descriptions of two practical applications of mental health information systems in Connecticut and Pittsburgh. In both these cases legal measures are given prominence. In Pittsburgh, officials wanted to adapt the Drug and Alcohol Abuse Control Act, to maintain stringent standards for the confidentiality of psychiatric records. The Act restricts disclosure of any record without client consent and provides access to medical personnel only for diagnosis or treatment, and to government officials for obtaining benefits due the client. In Connecticut, the hospital was using the Multi-State Information System, which was protected by a special statute, Section 79(J) of the Civil Rights Law of the State of New York. Descriptions of two exemplary Systems in Saskatchewan (D'Arcy, 1983) and Alberta (Wolfus and Bland, 1983) also Suggest many policies. In the Saskatchewan system, all the hospital staff were subject to an oath of office whose violation was a criminal offense. Codes and passwords were used to limit access and system users in one region can only have information from their region. The central office could have access to overall aggregate information, but without client identifiers. External requests were approved by a separate Data Release Committee. The Alberta system has more hardware and software measures to protect the privacy of clients. Each terminal has a unique code which needs to be entered to gain access, and each user has a special user number which also needs to be entered. Also, each clinic will have access to information only from their location.

Very recently, the "Computer-based Patient Record Institute" (CPRI) has been created by the representatives of leading medical, hospital, insurance, nursing, technology and information groups and associations (Milholland and Heller, 1992). One of the chief objectives of CPRI is to create better policies and techniques to protect client and provider confidentiality and ensure data security.

SUMMARY

The issue of privacy of information, as it relates to physician-client relationships, has been stressed since the time of Hippocrates 2400 years ago (Schuchman, 1980). However, these foundations of privacy have recently come under additional scrutiny due to two significant factors: 1) the rise in the use of computer technology, and 2) the increasing demands by third parties like insurance payers, governmental bodies and the legal system for privileged data (Schuchman, 1980; Nye, 1980).

Computerized data collection, storage and retrieval facilitate locating and obtaining

personal information. "Knowledge of a person's intimate facts effectively places the individual, his or her family, business, and personal future in the hands of the knower. (Nye, 1980. p.650) This leads to mistrust of medical information systems, among the public. The degrees of concern increases significantly with respect to mental health data, due to the stigma of mental illness that is pervasive in this society. To address these concerns, and fully utilize mental health information systems, various technical, organizational and legal measures can be used. These measures can safeguard client privacy and maintain confidentiality of sensitive information. The proposed nationwide network of patient records will have three levels of security based on the type of data. The highest level of security is for extremely sensitive data that includes psychiatric history (Larkin, 1991).

Westin (1976), has proposed 12 principles that cover various aspects of data collection and management of medical information.

1. Requiring public notice of the creation of any automated data system containing identified health records.
2. Setting limits on collection and recording of personal health data based on standards of relevance and propriety.
3. Notifying individuals as to how information will be used, procedures for consent, and policies regarding disclosure.
4. Requiring that data release forms be specific as to date disclosed, to whom and for what purpose, and that release consent be informed.
5. Enabling client access to their own information.
6. Imposing upon data collectors a duty to insure accuracy.
7. Imposing upon the data system the duty to apply appropriate security measures.
8. Imposing upon the data system a duty of education and information to inculcate respect for citizen rights.
9. Requiring the data system to prepare a patients' rights handbook and offer a patients' rights representative.
10. Establishing independent audit and periodic review of data and data collection.
11. Developing techniques for public oversight of health care consistent with the protection of personal privacy.
12. Establishing appropriate guidelines for the use of health care data in necessary research and program evaluations.

These principles may provide overall guidelines for designing and implementing mental health information Systems without endangering client privacy and confidentiality of information.

BIBLIOGRAPHY

Alexander, Mary Jane, Carole Siegel, and Chris Murtaugh, 1985. "Automating the psychiatric record for care review purposes: A feasibility analysis." Computers in Human Services, 1(4):1-16.

American Health Information Management Association, 1993. Health Information Model Legislation Language. Washington, DC.

American Medical Association. 1976. "A.M.A. model state bill on confidentiality of health care information." Pp.350~356 In A.F. Westin, Computers, Health Records, and Citizen Rights. National Bureau of Standards Monograph No.157. Washington, D.C.: U.S. Government Printing Office.

Anderson, J. 1977. "Realization of data protection in health information systems." Pp.7-13 In G. Griesser (ed), Realization of Data Protection in Health Information Services. Amsterdam: North-Holland Publishing.

Aydin, C.E. 1989. "Occupational adaptation to computerized medical information systems." Journal of Health and Social Behavior, 30(2):163-179.

Bank, Rheta and Eugene M. Laska, 1978. "Protecting privacy and confidentiality in a multiple use, multiple user mental health information system." Evaluation and Program Planning, 1(2):151-157.

Bank, Rheta 1981. "Legal issues surrounding psychiatric records." Pp.245-260 In C. Siegel and S. Krupnick Fischer (eds), Psychiatric Records In Mental Health Care. New York: Brunner/Mazel Publishers.

Baskin, David.,and Samuel Seiffer. 1990. "A nationwide survey of computer utilization in community mental health centers." p.159-170 In D.Baskin (ed), Computer Applications in Psychiatry and Psychology. New York: Brunner/Mazel ,Inc.

Baskin, David (ed). 1990. Computer Applications in Psychiatry and Psychology. New York: Brunner/Mazel, Inc.

Bennett, Edward M., and Barry Trute, (eds). 1983. Mental Health Information System: Problems and Prospects. New York: The Edwin Mellen Press.

Binner, Paul R. 1988. "Mental health management decision making in the age of the computer." Computers in Human Services, 3:87-100.

Biskup, J. 1990. "Protection of privacy and confidentiality in medical information systems: problems and guidelines." Pp.13~3 In D. Spooner and C. Landwehr (eds), Database Security III. Status and Prospects. New York: North-Holland Publishing.

Bloum, A.G., E.L. Perez, and J.H. Bloum, 1988. "Computerized Administration of the

diagnostic interview schedule." Psychiatry Research, 23(3) :335-344.

Bruce, Jo Anne C. 1984. Privacy and Confidentiality of Health Care Information. Chicago: American Hospital Publishing.

Campbell, Givner N., C.B. Seelig, A.L. Greer. 1989. "Computerized medical records and clinic function." Medical Computing, 6(5):282-287.

Chapman, R.L. 1976. The Design for Management Information Systems for Mental Health Organizations: A Primer. (NIMH Series FN No.5). Washington, D.C.: U.S. Government Printing Office.

Conference on User-Oriented Mental Health Information Systems: A Report, April 1975. [NIMH. ADM42-74-90(OP)]. Atlanta, Ga.: Southern Regional Education Board.

Curran, William J. and Rheta Bank. 1975. "The multistate information system and confidentiality and privacy protection." Pp.405-445 In E.M. Laska and R. Bank (eds), Safeguarding Psychiatric Privacy: Computer Systems and Their Uses. New York: John Wiley and Sons.

D'Arcy, Carl. 1983. "The Saskatchewan mental health information system: exposition and comment." Pp.131-150 In E.M. Bennett and B. Trute (eds), Mental Health Information Systems: Problems and Prospects. New York: The Edwin Mellen Press.

DeTore, A.W. 1988. "Medical informatics: An introduction to computer technology in medicine." American Journal of Medicine, 85(3):399-403.

Dick, R.S. and E.B. Steen (eds). 1991. The Computer Based Patient Record: An Essential Technology For Health Care. Washington, D.C.: National Academy Press.

Dickens, Bernard M. 1983. "Political and legal considerations." Pp.99-120 In E.M. Bennett and B. Trute (eds), Mental Health Information Systems: Problems and Prospects. New York: The Edwin Mellen Press.

Dowling, A.F. Jr. 1989. "Health care information Systems architecture of the near future." Journal of Social HealthSystems, 1(2):77-97.

Finn, Jerry. 1990. "Security, privacy, and confidentiality in agency microcomputer use." Families in Society, 1(5):283-290.

Gandy, Oscar H. 1989. "The surveillance society: Information technology and bureaucratic social control." Journal of Communication, 39:61-76.

Grady, C., C. Romano, and J. Jacob. 1991. "Confidentiality: A survey in a research hospital." Journal of Clinical Ethics, 2(1):25-30.

Greist, John H. 1990. "Computers and psychiatric diagnosis." Pp.2142 In D. Baskin (ed), Computer Applications in Psychiatry and Psychology. New York: Brunner-Mazel, Inc.

Greist, John H. 1988. "Computers in clinical psychiatry." Psychiatric Annals, 18(4):207-208.

Griesser, G.G. (ed). 1980. Data Protection In Health Information Systems: Considerations and Guidelines. International Medical Informatic Association Working Group 4. Amsterdam: North-Holland Publishing.

Griesser, G. 1985. "The issue of data protection in computer-aided health care information systems". Pp.113-117 In K.J. Hannah, E. J. Guillemin and D.N. Conklins (eds), Nursing Uses of Computers and Information Science. North-Holland: Elsevier Science Publishers.

Harvey, Williard J. 1988. "Data and data bases." Pp.69-83 In C.J. Austin (ed), Information Systems for Health - Administration. (3rd Ed). Ann Arbor, Michigan: Health Administration Press.

Hedlund, James L. 1978. "Mental Health Information Systems: Some national trends." Pp.109-116 In F.H. Orthner (ed), Proceedings of the Second Annual Symposium on Computer Applications in Medical Care. New York: Institute of Electrical and Electronic Engineers.

Hedlund, James L., B.W. Vieweg, D.W. Cho. 1985. "Mental health computing in the 1980's: Clinical Applications." Computers in Human Services, 1(2):1-31.

Hedlund, James L., B.W. Vieweg, D.W. Cho. 1985. "Mental health computing in the 1980's: General information systems and clinical documentation". Computers in Human Services, 1(1):3-33.

Hedlund, J.L., B.W. Vieweg, J.B. Wood, D.W. Cho, R.C. Evenson, C.V. Hickman, and R.A. Holland. 1981. Computers in Mental Health: A Review and Annotated Bibliography. (NIMH Series FN No.7; DHHS Publication Number (ADM)81-1090). Washington, D.C.: U.S.Government Printing Office.

Hedlund, J.L. and B.W. Vieweg. 1982. "Some utilization and maintenance issues with mental health information systems." Pp.130-134 In B.I. Blum (ed), Proceeding of the Sixth Annual Symposium on Computer Applications in Medical Care. New York: Institute of Electrical and Electronic Engineers.

Hedlund, James L. 1988. "Mental health computing in Great Britain." Computers in Human Services, 3:5-27.

Hedlund, J.L., I.W. Sletter, and R.C. Evenson. 1977. "Automated psychiatric information systems: A critical review of Missouri's standard system of psychiatry (SSOP)." Journal of Operational Psychiatry, 8:5-26.

Hiller, M.D. and L.F. Seidel. 1982. "Patient-care management Systems, medical records, and privacy: A balancing act." Public Health Reports, 97(4):332-345.

Hofftmann, L.J. 1977. Modern Methods For Computer Security and Privacy. Englewood Cliffs, N.J.: Prentice-Hall.

Hogan, Michael F., and Susan M. Essock. 1991. "Data and decisions: Can mental health management be knowledge-based?." Journal of Mental Health Administration, 18(1):12-20.

Katz, James F. 1990. "Public opinion trends: Privacy and information technology: The polls- a report." Public Opinion Quarterly, 54:125-143.

Knesper, D.J., G.C. Quarton, M.J. Gorodezky, and C.W. Murray. 1978. "A survey of the users of a working state mental health information system: Implications for the development of improved systems." In F.H. Orthner (ed), Proceedings of the Second Annual Symposium On Computer Applications in Medical Care. New York: Institute for Electrical and Electronic Engineers.

Koch, Edward I. 1975. "Right to privacy." Pp.401-404 In F.M. Laska and R. Bank (eds), Safeguarding Psychiatric Privacy: Computer Systems and Their Uses. New York: John Wiley and Sons.

Kupfer, David J, Michael Levine, and John A. Nelson. 1976. Mental Health Information Systems: Design and Implementation. New York: Marcel Dekker, Inc.

Lanman, Robert B. 1980. "The federal confidentiality protection for alcohol and drug abuse patient records: A model for mental health and other medical records?" American Journal of Orthopsychiatry, 50(4):666-77.

Larkin, H. 1991. "Network of computerized patient records seen ahead", American Medical News, 34:9-10.

Laska, Eugene. 1981. "Developments in computerization of the psychiatric record." Pp.271-282 In C. Siegel and S. Krupnick Fischer (eds), Psychiatric Records In Mental Health Care. New York: Brunner/Mazel Publishers.

Laska, E.M., C. Siegel, M. Meisner, R. Bank, and B. Zeitz. 1975. "Data Systems and mental health: Recommendations to the W.H.O." Pp.381-390 In E.M. Laska and R. Bank (eds), Safeguarding Psychiatric Privacy: Computer Systems and Their Uses. New York: John Wiley and Sons.

Laska, Eugene M. and Rheta Bank (ed). 1975. Safeguarding Psychiatric Privacy: Computer Systems and Their Uses. New York: John Wiley and Sons.

Leginski, Walter A., C. Croze, I. Driggers, S. Dumpman, D. Geertsen, E. Kamis-Gould,

M.J. Namerow, R.E. Patton, N.Z. Wilson, and C. Wurster. 1989. Data Standards for Mental Health Decision Support Systems. (NIMH Series FN No.10; DHHS Publication Number (ADM)89-1589). Washington, D.C.: U.S. Government Printing Office.

McDonald, C.J. 1989. "Medical information systems of the future." Medical Computing, 6(2):82-87.

Mednick, Stuart E. 1982. "Management policies and procedures needed for effective computer security." Pp.161-181 In J.A. Worthley (ed), Managing Computers in Health Care: A Guide For Professionals. Ann Arbor, Michigan: AUPHA Press.

Mezzich, Juan E., and Ada C. Mezzich. 1988. "The place of computers in psychiatry." Pp.61-75 In J.G. Howells (ed), Modern Perspectives in Clinical Psychiatry. Modern perspectives in psychiatry, No.10. New York: Brunner/Mazel, Inc.

Milholland, Kathy D. and B.R. Heller. 1992. "Computer-based patient record: From pipe dream to reality." Computers in Nursing, 10(5): 191-192.

Nye, Sandra G. 1980. "Patient confidentiality and privacy: The federal initiative." American Journal of Orthopsychiatry, 50(4):649~58.

Paton, J.A. and P.K. D'huyvetter. 1980. Automated Management Information Systems for Mental Health Agencies: A Planning and Acquisition Guide. (NIMH Series FN No.1; DHHS Publication Number 80-797). Washington, D.C.: U.S. Government Printing Office.

Peterson, H. and D. Fenna. 1977. "Data protection by software techniques with special regard to problems created by multi-user access." Pp.83-87 In G. Griesser (ed), Realization of Data Protection In Health Information Systems. Amsterdam: North-Holland Publishing Co.

Plutchik, Robert, and Toksoz B. Karasu. 1990. "Computers in interviewing and psychotherapy." Pp.57-76 In D. Baskin (ed), Computer Applications in Psychiatry and Psychology. New York: Brunner/Mazel, Inc.

Pollack, Daniel 1991. "Sharing information without forsaking personal privacy." Corrections Today, 53:30-32.

Privacy Protection Study Commission. 1977. Personal Privacy in an Information Society. Washington,D.C.: U.S. Government Printing Office.

Regan, Priscilla M. 1986. "Privacy, government information and technology." Public Administration Review, 46:629~34.

Reichert:, P.L. 1977. "Realization of data protection by software techniques." Pp.89-95 In G.Griesser (ed), Realization of Data Protection in Health Information Services. Amsterdam: North-Holland Publishing.

Rittman, Maude R. and R. H. Gorman. 1992. "Computerized databases: Privacy issues in the development of the Nursing Minimum Data Set." Computers In Nursing, 10(1):14-18.

Robinson, James 1990. "Use of computers in mental health management of information." Pp.111-124 In D.Baskin (ed), Computer Applications in Psychiatry and Psychology. New York: Brunner/Mazel, Inc.

Romano, Carol A. 1987. "Privacy, confidentiality, and security of computerized systems." Computers In Nursing, 5(3):99-104.

Sauter, K. 1977. "Data protection by software techniques with special regard to problems created by multi-user access." Pp.97-105 In G. Griesser (ed), Realization of Data Protection In Health Information Systems. Amsterdam: North-Holland Publishing Co.

Schmauss, Diane. 1991. "Computer security and data confidentiality." AORN Journal, 54(4):885-890. Scholes, M. 1986. "Computers in nursing. Private and confidential." Nursing Times, 82(13):59-60.

Schuchman, Herman. 1980. "Confidentiality: Practice issues in new legislation." American Journal of OrthoDpsychiatry, 50(4): 641~8.

Schwartz, Marc D. 1990. "Mental health computing: Directions for research." Pp.11-19 In D. Baskin (ed), Computer Applications in Psychiatry and Psychology. Clinical and experimental psychiatry, monograph No.2. New York: Brunner-Mazel, Inc.

Schwartz, Marc D. 1984. "Guidelines for user access to computerized patient records (a review)." Pp.479~80 In M.D. Schwartz (ed), Using Computers in Clinical Practice:Psychotherapy and Mental Health Annlications. New York: The Haworth Press.

Schwartz, Marc D. (ed). 1984. Using Computers in Clinical Practice: Psychotherapv and Mental Health Applications. New York: The Haworth Press.

Searcy, Larry L. 1984. "Issues in the development of a community-wide mental health information system." Pp.285-297 In M.D. Schwartz (ed), Using Computers in Clinical Practice: Psychotherapy and Mental Health Applications. New York: The Haworth Press.

Sherman, Paul S. 1987. "Administration/management issues in mental health computer applications." Computers in Human Services, 2:131-144.

Sidowski, J.B., J.H. Johnson, and T.A. Williams (eds). 1980. Tecbnoogy In Mental Health-Care Delivery Systems. Norwood, N.J.: Ablex.

Snyder, Richard. 1986. "Computerization in a mental health center." Computers in Psvchiatrv/Psvchology, 7(4):23-24.

Till, James E. and Gerrit De Boer. 1983. "Use of an information system to foster research." Pp.249-262 In E.M. Bennett and B.Trute (eds), Mental Health Information System: Problems and Prospects. New York: The Edwin Mellen Press.

Ting, T.C. 1990. "Application information security semantics: A case of mental health delivery." Pp.1-12 In D. Spooner and C. Landwehr (eds), Database Security III, Status and Prospects. New York: North-Holland Publishing.

Trute, Barry, Bruce Teffi, David Scuse, (eds). 1985. Human Service Information Systems: How To Design and Implement Them. Leviston, New York: The Edwin Mellen Press.

Ware, Willis. 1976. "Privacy Definitions." Pp.348-349 In A.F. Westin, Computers, Health Records, and Citizen Rights. National Bureau of Standards Monograph No.157. Washington, D.C.: U.S. Government Printing Office.

Westin, Alan F. 1982. "Patient's rights: Computers and health records." Pp.198-209 In J.A. Worthley (ed), Managing Computers in Health Care: A Guide For Professionals. Ann Arbor, Michigan: AUPHA Press.

Westin, A.F. and F. Isbell. (ed). 1977. A Policy Analysis of Citizen Rights Issues in Health Data Systems. National Bureau of Standards; Special Publication 469.

Westin, Alan P.1976. Computers, Health Records, and Citizen Rights. National Bureau of Standards Monograph No.157. Washington, D.C.: U.S. Government Printing Office.

Westin, Alan F. 1975. "Legal measures on national levels to protect privacy and confidentiality." Pp.365-379 In E.M. Laska and R. Bank (eds), Safeguarding Psychiatric Privacy: Computer Systems and Their Uses. New York: John Wiley and Sons.

Wolfus, Beverly, and R.C. Bland. 1983. "The Alberta Health information System." Pp.151-168 In E.M. Bennett and B.Trute (eds), Mental Health Information Systems: Problems and Prospects. New York: The Edwin Mellen Press.

Wolkon, G.H., and M. Lyon. 1986. "Ethical issues in computerized mental health data systems." Hospital and Community Psychiatry, 37(1):11-12,16.

Worthley, John A. 1982. "Maintaining information privacy." Pp.189-197 In J.A. Worthley (ed), Managing Computers in Health Care: A Guide For Professionals. Ann Arbor, Michigan: AUPHA Press.

Wurster, C.R. and J.D. Goodman. 1980. "NIMH Prototype management information system for community mental health centers." in J.T. O'Neill (ed), Proceedings of the Fourth Annual Symposium on Computer Applications in Medical Care. New York: Institute for Electrical and Electronic Engineers.

Young, Randy. 1982. "Your health, their business." Pp.210-215 In J.A. Worthley (ed), Managing Computers in Health Care: A Guide For Professionals Ann Arbor, Michigan:

AUPHA Press.

Zawadski, Rick T. 1984. "A practical guide to integrated computerized information management." Pp.273-284 In M.D. Schwartz (ed), Using Computers in Clinical Practice: Psychotherapy and Mental Health Applications. New York: The Haworth Press.

Zieseri, R.M, and S.P. Dowell. 1989. "Using microcomputers to improve the timeliness, accuracy, and accessibility of clinical data." Journal of Social Health Systems, 1(2):12-24.

Ziglin, Alan L. Reporting Requirements and MHSIP: The Appropriate Relationship Between Accountability and Data Standards for Decision Support Systems. Unpublished document prepared for the National Institute of Mental Health. August, 1991.

APPENDIX B

METHODOLOGY

Project Methodology

This project began as a Technical Assistance request to the National Institute of Mental Health which is now the Center for Mental Health Services. This request arose out of the concerns of the Nebraska Department of Public Institutions that, despite the importance of the topic of confidentiality and appropriate uses of data, no known comprehensive effort had addressed this topic. A key component to the Technical Assistance request was that the product, in addition to meeting the needs of Nebraska, would potentially be useful to other states, regions or programs.

As proposed, the project began at the National Conference on Mental Health Statistics in 1992. Relevant sessions were attended by the project consultant and numerous individual conversations were held attempting to assure that this technical assistance activity would be responsive to the needs throughout the nation, and not just to one state. Following the conference, several key individuals around the country who are involved in this area were contacted and their insights solicited.

The next step was to conduct a literature review (see Appendix A). The main focus was on books and journal articles published since 1975. The purpose of this review was to assure that this technical assistance project was prepared to build on previous efforts, as opposed to "reinventing the wheel".

Following the literature review, a Task Force comprised of persons from Nebraska was convened. The Task Force was to provide input into the project. Its membership was to be a broad cross section of persons who were stakeholders in the mental health service delivery system. Among the members were current or former clients, advocates, local providers, state administrators, potential data users from academia, and others. The Task Force provided input through meetings as well as through feedback to materials provided them by mail.

It was interesting to note that while the original request for technical assistance included an outline of topics to be covered, this material was not shared with the Task Force members prior to their first meeting. This was done in an effort to avoid "imprinting" or limiting the range and content of their input. However, when reviewed, the material generated by the first meeting fit well into the outline earlier proposed. This is taken as an indication that the technical assistance effort is needed and has properly focused on significant unresolved issues for constituents of the public sector mental health system.

Finally, a draft of the deliverable product of this Technical Assistance Project formed the basis of a Roundtable discussion at the 1994 National Conference on Mental Health Statistics. This session provided additional input into the final product of this project.

APPENDIX C

ILLUSTRATIVE EXAMPLES OF ETHICAL ISSUES

Illustrative Examples of Ethical Issues

Illustrative examples of ethical issues include:

-If assassination threats are made against high level elected official',, should the database be used to locate the person making such threats and thus potentially avoid an assassination? Requests may be made to use automated clinical records to gain an indication of the seriousness of such threats.

-Should automated records from mental health programs be used to help locate persons who are violating court orders by not contributing to the support of their children?

-Another scenario might involve a small rural community which is displeased with the local mental health program because it is alleged that a client is supporting himself or herself by illegally selling controlled medications which are prescribed by the program and provided at minimal cost through their pharmacy. If the program does not have a positive image in the community, it cannot reach all the persons it is thereto serve. Would it be acceptable to use the data base in order to determine that the person alleged to be selling the medication had never been a client at the program, or had been a client but had never been prescribed the medication which was involved in the allegation?

-Hargrove (1986) argues that these ethical issues are especially sensitive in rural areas. Does this mean that data access should be controlled not only on the basis of "need to know", but also on the basis of geography?

Other examples of ethical issues include:

-The fact of life is that bureaucracies must operate within strict budgetary limitations. How does one decide how much of the limited resources are to be utilized in order to store the data in a manner which assures what level of protection?

-Another ethical issue is that electronic transmission of data (either computer-to-computer, or by facsimile machine) increases the possibility of violation of confidentiality. This violation can be either intentional or accidental. However, the client may have authorized such release and prompt transmission may be in the best interest of the client. Since the client has authorized the electronic transfer of data, the dilemma here is not whether electronic transmission is acceptable. The issue is who is to decide if the safeguards are adequate to assure that the risk is acceptably low.

-Gulbinat (1994) raises many interesting ethical issues. In one case he states ~. 39) that it, "...is clear that the potential for a rational organization of data in mental health information systems does not itself provide any legal, let alone ethical justification for the storage, transmission and use of patient related data. Nevertheless, it may well be argued that it would be unethical not to take advantage of the possible benefits that mental health information systems offer."

-In another example, Gulbinat (1994) points out ~. 41) that little, "...attention has been given to whether it is ethical for patients to refuse consent for their data to be entered into a computer-based information system, or to refuse the use of such data for anything but their own treatment in a narrow sense." He then goes on to ask, "...it

ethical to take advantage of the latest research findings for one's own treatment, but refuse to contribute one's data to the furthering of mental health research, to the benefit of the group of all patients to which one belongs?"

-Finally, not all ethical issues are client oriented. Some surround service providers. For example, when can, or should, a provider share data with another provider:

- within the same mental health program?
- in another mental health program?
- in another human service agency?

APPENDIX D

DRAFT MODEL LEGISLATION

American Health Information Management Association
1225 I St., N.W.
Washington, DC 20005
(202) 218-3535

Feb.1993

AMERICAN HEALTH INFORMATION MANAGEMENT ASSOCIATION

HEALTH INFORMATION MODEL LEGISLATION LANGUAGE

SEC. 101. PREAMBLE

The Congress finds that:-

(a) The right of privacy is a personal and fundamental right protected by the Constitution of the United States:

(b) Health care information is personal and sensitive information that, if improperly used or released, may do significant harm to a patient's interest in privacy and in health care, and may affect a patient's ability to obtain employment, education, insurance, credit, and other necessities;

(c) Patients need access to their own health care information as a matter of fairness to enable them to make informed decisions about their health care and correct inaccurate or incomplete information about themselves;

(d) Persons maintaining health care information need clear and certain rules for the disclosure of health care information;

(e) Persons other than health care providers obtain, use, and disclose health care information in many different contexts and for many different purposes. A patient's interest in the proper use and disclosure of the personal health care information continues even when the information has been initially disclosed and is held by persons other than health care providers; and

(f) The movement of patients and their health care information across state lines, access to and exchange of health care information from automated data banks and networks and the emergence of multi-state health care providers and payors creates a compelling need for Federal law, rules and procedures governing the use and disclosure of health care information.

SEC. 102. GENERAL DEFINITIONS.

In this [Act] (except as otherwise provided).

(a) AUDIT - The term "audit" means an assessment, evaluation, determination, or investigation of a person maintaining health care information or health care rendered by such a person by a person not employed by or affiliated with the person audited to determine compliance with--

(1) statutory, regulatory, fiscal, administrative, medical, or scientific

standards;

(2) the requirements of a private or public program of payment for health care; or

(3) requirements for licensure, accreditation, or certification.

(b) **COMPULSORY DISCLOSURE** -- The term "compulsory disclosure means any disclosure of health care information mandated or required by Federal or State law in connection with a judicial, legislative, or administrative proceeding. including but not limited to, disclosure required by subpoena, subpoena duces tecum, request or notice to produce, court order, or any other method of requiring a person maintaining health care information to produce health care information under the criminal or civil discovery laws of any State or Federal government or administrative agency thereof.

(c) **HEALTHCARE** -- The term "health care" means:-

(1) any preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, counseling, service, or procedure provided by a health care provider:-

(A) with respect to a patient's physical or mental condition, or

(B) affecting the structure or function of the human body or any part thereof, including, but not limited to, banking of blood, sperm, organs, or any other tissue; and

(2) any sale or dispensing of any drug, substance, device, equipment, or other item to a patient or for a patient's use, pursuant to a prescription.

(d) **HEALTH CARE INFORMATION** -- The term "health care information" means any data or information whether oral or recorded in any form or medium, that identifies or can readily be associated with the identity of a patient or other record subject; and

(1) relates to a patient's health care; or

(2) is obtained in the course of a client's health care from a health care provider, from the patient, from a member of the patient's family or an individual with whom the patient has a close personal relationship, or from the patient's legal representative.

(e) **HEALTH CARE PROVIDER** -- The term "health care provider" means a person who is licensed, certified, registered or otherwise authorized by law to provide health care in the ordinary course of business or practice of a profession.

(f) INSTITUTIONAL REVIEW BOARD -- The term "review board" means any board, committee, or other group formally designated by an institution, or authorized under Federal or State law, to review, approve the initiation of, or conduct periodic review of, research programs to assure the protection of the rights and welfare of human research subjects.

(g) MAINTAIN -- The term "maintain," as related to health care information, means to create, collect, handle, hold, possess, preserve, retain, store, control or transmit such information.

(h) PATIENT.-The term "patient" means an individual who receives or has received health care. The term includes a deceased individual who has received health care.

(i) PATIENT'S AUTHORIZATION -- The term "patient's authorization" means an authorization that is valid under the provisions of Section 104.

(j) PATIENT REPRESENTATIVE -- The term "patient representative" shall mean any individual legally empowered to make decisions concerning a patient's health care or the administrator or executor of a deceased patient's estate.

(k) PERSON -- The term "person" means--

(1) an individual, corporation, business trust, estate, trust, partnership, association, joint venture, or any other legal or commercial entity; and

(2) except for purposes of Section 111 and 112, a government, governmental subdivision, agency or authority.

(l) SECRETARY -- The term "Secretary" means the Secretary of health and Human Services.

SEC. 103. DISCLOSURE.

(a) DISCLOSURE -- No person other than a patient or patient representative may disclose health care information to any other person without the patient's authorization, except as authorized in Section 105. No person may disclose health care information under a patient's authorization, except in accordance with the terms of such authorization. The provisions of this paragraph shall apply both to disclosures of health care information and to redisclosures of health care information by a person to whom health care information is disclosed.

(b) RECORD OF DISCLOSURE -- Each person maintaining health care information shall maintain a record of all external disclosures of health care information made by such person concerning each patient, and such record shall become part of the health care information concerning each patient. The record of each disclosure shall include the name, address and institutional affiliation, if any, of the person to

whom the health care information is disclosed, the date, and purpose of the disclosure and, to the extent practicable, a description of the information disclosed.

SEC. 104. PATIENT'S AUTHORIZATION; REQUIREMENTS FOR VALIDITY.

(a) To be valid, a patient's authorization must-

- (1) Identify the patient;
- (2) Generally describe the health care information to be disclosed;
- (3) Identify the person to whom the health care information is to be disclosed;
- (4) Describe the purpose of the disclosure;
- (5) Limit the length of time the patient's authorization will remain valid;
- (6) Be given by one of the following means-
 - (A) In writing, dated and signed by the patient or the patient representative; Or
 - (B) In electronic form, dated and authenticated by the patient or the patient representative using a unique identifier, and

(7) Not have been revoked under paragraph (b).

(b) REVOCATION OF PATIENT'S AUTHORIZATION -- A patient or patient's representative may revoke the patient's authorization at any time, unless disclosure is required to effectuate payment for health care that has been provided to the patient, or other substantial action has been taken in reliance on the patient's authorization. A patient may not maintain an action against a person for disclosure of health care information made in good faith reliance on the patient's authorization, if the person had no notice of the revocation of the patient's authorization at the time disclosure was made.

(c) RECORD OF PATIENT'S AUTHORIZATIONS AND REVOCATIONS -- Each person maintaining health care information shall maintain a record of all patient's authorizations and revocations thereof, and such record shall become part of the health care information concerning each patient.

(d) NO WAIVER -- Except as provided by this [Act], the signing or authentication of an authorization by a patient or patient representative is not a waiver of any rights a patient has under other Federal or State statutes, the rules of evidence, or common law.

SEC. 105. DISCLOSURE WITHOUT PATIENT'S AUTHORIZATION.

A person maintaining health care information may disclose health care information about a patient without the patient's authorization as follows:-

(a) DISCLOSURE TO THE PATIENT OR PATIENT REPRESENTATIVE -- Any disclosure or patient information to the patient or such patient's patient

representative;

(b) DISCLOSURE BY FAMILY AND FRIENDS -- Any disclosure of health care information by a family member or by any other individual with whom the patient has a personal relationship, provided that:-

(1) the health care information was disclosed to such individual by the patient or otherwise not in violation of this [Act]; and

(2) the health care information was not disclosed to the individual making the disclosure in the course of providing health care to the patient;

(c) DISCLOSURE TO EMPLOYEES AND AGENTS -- disclosure, to the extent necessary for the disclosing person to carry out its lawful activities, to the disclosing person's agent employee, or independent contractor who is under a legal obligation to hold the health care information in confidence and not to use such health care information for any purpose other than the lawful purpose for which the health care information was obtained by the disclosing person;

(d) DISCLOSURE TO ANOTHER HEALTH CARE PROVIDER -- Disclosure to a health care provider who is providing health care to the patient except as such disclosure is limited or prohibited by the patient;

(e) DISCLOSURE TO AVOID DANGER -- Disclosure to any person to the extent the recipient needs to know the information, if the person holding the health care information reasonably believes that such disclosure will avoid or minimize imminent danger to the health or safety of the patient or any other individual, or is necessary to alleviate emergency circumstances affecting the health or safety of any individual;

(f) DISCLOSURE TO FAMILY -- Disclosure to a member of the patient's immediate or to any other individual with whom the patient is known to have a close personal relationship, if such disclosure is made in accordance with good medical or other professional practice, except as such disclosure is limited or prohibited by the patient;

(g) DISCLOSURE TO SUCCESSOR IN INTEREST -- Disclosure to a person who is a successor in interest to the person maintaining the health care information, provided, however, that no person other than a licensed health care provider or the spouse of a deceased health care provider shall be considered a successor in interest to a health care provider;

(h) DISCLOSURE TO GOVERNMENTAL AUTHORITIES -- Disclosure to Federal, State, or local governmental authorities, to the extent the person holding the health care information is required by law to report specific health care information:-

(1) when needed to determine compliance with State or Federal licensure

certification, or registration rules or law; or

(2) when needed to protect the public health;

(i) DISCLOSURE FOR AUDITS -- Disclosure to a person who obtains health care information solely for purposes of an audit, if that person agrees in writing:-

(1) to remove from the health care information or destroy, at the earliest opportunity consistent with the purpose of the audit, information that would enable identification of the patient;

(2) not to disclose in any public report any medical information; and

(3) not to further disclose the health care information except to accomplish the audit or to report unlawful or improper conduct involving health care payment fraud by a health care provider or a patient or other unlawful conduct by the healthcare provider;

(j) DISCLOSURE FOR RESEARCH -- disclosure for use in a research project.

(1) that an institutional review board has determined:-

(A) is of sufficient importance to outweigh the intrusion into the privacy of the patient that would result from the disclosure;

(B) is reasonably impracticable without the use of disclosure of the health care information in individually identifiable form;

(C) contains reasonable safeguards to protect the information from redisclosure;

(D) contains reasonable safeguards to protect against identifying, directly indirectly, any patient in any report of the research project; and

(E) contains procedures to remove or destroy at the earliest opportunity, consistent with the purposes of the project, information that would enable identification of the patient, unless the institutional review board authorizes retention of identifying information for purposes of another research project; and

(2) If the person agrees in writing:-

(A) to remove from the health care information or destroy, at the earliest opportunity consistent with the purpose of the research project, information that would enable identification of the patient;

(B) not to disclose health care information in any public report, and

(C) not to further disclose the health care information, except as necessary to conduct the research project approved by the institutional review board.

(k) COMPULSORY DISCLOSURE -- Compulsory disclosure in accordance with the requirements of Section 108;

(l) DISCLOSURE TO LAW ENFORCEMENT BY A COURT -- Disclosure to Federal, State or local law enforcement authorities to the extent required by law;

(m) DISCLOSURE DIRECTED BY A COURT -- disclosure directed by a court in connection with a court-ordered examination of a patient; or

(n) DISCLOSURE TO IDENTIFY A DECEASED INDIVIDUAL -- Disclosure based on reasonable grounds to believe that the information is needed to assist in the identification of a deceased individual.

SEC. 106. STANDARDS FOR INFORMATION PRACTICES.

(a) PROMULGATION OF REQUIREMENTS --

(1) IN GENERAL -- Between July 1, 1994, and July 1, 1995, the Secretary shall promulgate requirements for information practices of persons maintaining health care information. Such requirements shall be consistent with the provision of this Act] and shall be in accordance with the principles set forth in paragraph (b).

(2) REVISION -- The Secretary may from time to time revise the requirements promulgated under this paragraph.

(b) PRINCIPLES OF FAIR INFORMATION PRACTICES -- The requirements promulgated in this paragraph (a) shall incorporate the following principles:

(1) PATIENTS RIGHT TO KNOW -- The patient or the patient representative has the right to know that health care information concerning the patient is maintained by any person and to know for what purposes the health care information is used;

(2) RESTRICTIONS ON COLLECTION -- Health care information concerning a patient must be collected only to the extent necessary to carry out the legitimate purpose for which the information is collected;

(3) COLLECTION AND USE ONLY FOR LAWFUL PURPOSE -- Health care information must be collected and used only for a necessary and lawful purpose;

(4) NOTIFICATION TO PATIENT. Each person maintaining healthcare information must prepare a formal, written statement of the information priorities observed by such person. Each patient who provides health care information directly to a person maintaining health care information should receive a copy of the statement of the person's fair information practices and should receive an explanation of such fair information practices upon request;

(5) RESTRICTION OF USE FOR OTHER PURPOSES -- Health care information may not be used for any purposes beyond the purposes for which the health care information collected, except as otherwise provided in this (Act);

(6) RIGHT TO ACCESS -- The patient or the patient representative may have access health care information concerning the patient, has the right to have a copy of such healthcare information made after payment of a reasonable charge, and, further, has the right to have a notation made with or in such health care information of any amendment or correction of such health care information requested by the patient or patient representative;

(7) REQUIRED SAFEGUARDS -- person maintaining, using or disseminating health care information shall implement reasonable safeguards for the security of the health care information and its storage, processing and transmission, whether in electronic or other form;

(8) ADDITIONAL PROTECTIONS -- Methods to insure the accuracy, reliability, relevance, completeness, and timeliness of health care information should be instituted; and

(9) ADDITIONAL PROTECTIONS FOR CERTAIN HEALTH CARE INFORMATION -- If advisable, provide additional safeguards for highly sensitive health care information (such as health care information concerning mental health, substance abuse, communicable and genetic disease, and abortions, as well as health care information concerning celebrities and notorious individuals, and health care information contained in adoption records).

SEC. 107. OBLIGATIONS OF PATIENT REPRESENTATIVE.

(a) AUTHORITY OF PATIENT REPRESENTATIVES -- A person authorized to act as a patient representative may exercise the rights of the patient under this [Act] to the extent necessary to effectuate the terms or purposes of the grant of authority; but a patient who is a minor and who is authorized to consent to health care without the consent of a parent or legal guardian under State law may exclusively exercise the rights of a patient under this [Act] as to information pertaining to health care to

which the minor lawfully consented.

(b) GOOD FAITH OBLIGATION -- A patient representative shall act in good faith to represent the best interests of the patient with respect to health care information concerning the patient.

SEC. 108. COMPULSORY DISCLOSURE.

(a) LIMITS ON COMPULSORY DISCLOSURE -- No person may be compelled to disclose health care information maintained by such person pursuant to a request for compulsory disclosure in any judicial legislative or administrative proceeding, unless:

(1) The person maintaining the health care information has received a patient's, authorization to release the health care information in response to such request for compulsory disclosure;

(2) The patient has knowingly and voluntarily waived the right to claim privilege or confidentiality for the health care information sought;

(3) The patient is a party to the proceeding and has placed his or her physical or mental condition in issue;

(4) The patient's physical or mental condition is relevant to the execution or witnessing of a will;

(5) The physical or mental condition of a deceased patient is placed in issue by any person claiming or defending through or as a beneficiary of the patient:

(6) Health care information concerning the patient is to be used in the patient's commitment proceeding;

(7) The healthcare information is for use in any law enforcement proceeding or investigation in which a health care provider is the subject or a party; provided, however, that health care information so disclosed shall not be used against the patient, unless the matter relates to payment for the patient's health care or unless compulsory disclosure is ordered as authorized under subparagraph (9);

(8) The health care information is relevant to a proceeding brought under Section 110, 111, or 112; or

(9) The court or Federal or State agency or Congress or the State legislature has determined, after hearing any objections made pursuant to paragraph (d), that particular health care information is subject to compulsory disclosure

because the party seeking the health care information has demonstrated that the interest that would be served by disclosure outweighs the patient's privacy interests.

(b) NOTICE REQUIREMENT -- Unless the court, or Federal or State agency or Congress or State legislature, for good cause shown, determines that the notification should be waived or modified, if health care information is sought under subparagraph (2), (4) or (5), or in a civil proceeding or investigation pursuant to subparagraph (9), the person requesting compulsory disclosure shall serve upon the person maintaining the health care information and upon the patient's legal guardian or other person legally authorized to act for the patient in such a matter, or on the patient's attorney, the original or a copy of the compulsory disclosure request at least thirty (30) days in advance of the date on which compulsory disclosure is requested and a statement of the right of the patient and of the person maintaining the health care information to have any objections to such compulsory disclosure heard by such court, or governmental agency or Congress or State legislature prior to the issuance of an order for such compulsory disclosure and the procedure to be followed to have any such objection heard. Such service shall be made by certified mail, return receipt requested, or by hand delivery, in addition to any form of service required by applicable State or Federal law. The notice requirements of this paragraph shall not apply to a request for compulsory disclosure of health care information relating to a patient if made by or on behalf of a patient.

(c) CERTIFICATION UNDER OATH.

(1) A person seeking compulsory disclosure of health care information about a patient under this section shall provide the person maintaining the health care information from whom compulsory disclosure is sought with a written certification under oath by the person seeking such compulsory disclosure or an authorized representative of such person:-

(A) identifying each subparagraph of paragraph (a) under which compulsory disclosure of health care information is being sought; and

(B) stating that notice has been provided in accordance with the requirements of paragraph (b) or is not required by paragraph (b) with respect to any of the health care information sought.

(2) A person may sign a certification described in paragraph (1), only if the person reasonably believes that the subparagraph or subparagraphs of paragraph (a) identified in the certification provide an appropriate basis for the use of a request for compulsory disclosure.

(d) OBJECTION TO COMPULSORY DISCLOSURE -- If the person maintaining health care information for the patient or the patient's legal guardian or attorney or other person legally authorized to represent the patient in such a matter files in the

manner set forth in the notice described in paragraph (b) such person's objection to the request for compulsory disclosure prior to the date on which such compulsory disclosure is sought, the burden shall be on the person requesting such compulsory disclosure to seek an order from the appropriate court or Federal or State agency or State legislature or Congress an order compelling such disclosure, and the person or persons filing such objection may defend in any proceeding to compel such disclosure.

(e) MAINTENANCE OF NOTICE AND CERTIFICATION -- Unless otherwise ordered by the court, State or Federal agency, Congress or State legislature, a person maintaining health care information shall maintain a copy of each request for compulsory disclosure and accompanying certification as part of the patient's health care information.

(f) NO WAIVER -- Disclosure of health care information pursuant to compulsory disclosure, in and of itself, shall not constitute a waiver of any privilege, objection or defense existing under any other law or rule of evidence or procedure..

SEC. 110. CIVIL REMEDIES.

(a) PRIVATE RIGHT OF ACTION -- A person aggrieved by a violation of this [Act] may maintain an action for relief as provided in this section.

(b) JURISDICTION -- The district courts of the United States shall have jurisdiction in any action brought under the provisions of this section.

(c) RELIEF -- The court may order a person maintaining health care information to comply with this [Act] and may order any other appropriate relief.

(d) DAMAGES -- If the court determines that there is a violation of this [Act], the aggrieved person is entitled to recover damages for any losses sustained as a result of the violation; and, in addition, if the violation results from willful or grossly negligent conduct, the aggrieved person may recover not in excess of [\$10,000], exclusive of any loss.

(e) ATTORNEYS' FEES -- If a plaintiff prevails in an action brought under this section the court, in addition to any other relief granted under this section, may award the plaintiff reasonable attorneys' fees and all other expenses incurred by the plaintiff in the litigation.

(f) STATUTE OF LIMITATIONS -- Any action under this [Act] must be brought within two years from the date the alleged violation is discovered.

SEC. 111. CIVIL MONEY PENALTIES.

(a) Any person that knowingly discloses or health care information in violation of this [Act] shall be subject, in addition to any other penalties that may be prescribed by

law.

(1) to a civil money penalty of not more than [\$1,000] for each violation, but not to exceed [\$25,000] in the aggregate for multiple violations, except as provided in subparagraph (2); and, in addition

(2) to a civil money penalty of not more than \$1,000] if the Secretary finds that violations of this (Act] have occurred in such numbers or with such frequency as to constitute a general business practice.

SEC 112. CRIMINAL PENALTY FOR OBTAINING HEALTH CARE INFORMATION THROUGH FALSE PRETENSES OR THEFT.

(a) Any person who, under false pretenses or with a false or fraudulent certification required under this [Act], requests or obtains health care information maintaining health care information or a patient's authorization shall be fined not more than \$10,000 or imprisoned not more than six months, or both, for each offense.

(b) Any person, who, under false pretenses or with a fraudulent certification required under this [Act], requests or obtains health care information from a person maintaining health care information and who intentionally uses, sells or transfers such health care information for remuneration, or profit or for monetary gain shall be fined not more than \$50,000, or imprisoned for not more than two years, or both, for each offense.

(c) Any person who unlawfully takes health care information from a person maintaining health information and who intentionally uses, sells or transfers such health care information for remuneration, for profit or for monetary gain shall be fined not more than \$50,000, or imprisoned for not more than two years, or both, for each offense.

SEC. 113. PREEMPTION OF STATE LAWS.

(a) Effective as of the effective date of this [Act], no State may establish or enforce any law or regulation concerning the disclosure of health care information, except as provided in paragraph (b).

(b) This [Act] does not supersede any restriction on the disclosure or use of health care information under:-

(1) any Federal, or State law on the inspection of, or disclosure or use of health care information relating to alcohol or drug abuse, or health care for such abuse;

(2) any Federal, or State Law concerning the disclosure or use of health care information relating to psychiatric, psychological, mental health or

developmental disabilities health care;

(3) Section 1106 of the Social Security Act;

(4) Section 1160 of the Social Security Act; or

(5) any Federal or State law making information, including but not limited to health care information, that is maintained, used or generated in the course of peer review, quality assurance or similar activities or functions privileged or confidential.

(c) Nothing in this [Act] shall be construed to make any Federal Government authority or any Federal agency subject to any State or local law not otherwise applicable.

SEC. 114. MISCELLANEOUS PROVISIONS.

(a) SEVERABILITY -- If any provision of this [Act] or its application to any person or is held invalid, the invalidity does not affect other provisions or applications of this [Act] that can be given effect without the invalid provision or application, and to this end the provisions of this [Act] are severable.

APPENDIX E

ISSUES OF INFORMED CONSENT

CONFIDENTIALTY OF MEDICAL RECORDS AND CONSENT TO TREATMENT

**James L. Quinlan
Amy S. Bones
John M. Ryan**

**Fraser, Stryker, Vaughn, Meusey, Olson, Boyer & Bloch, P.C.
500 Energy Plaza
409 South 17th Street
Omaha, NE 68102**

**June 10, 1993
Cornhusker Hotel - Lincoln, Nebraska**

**Nebraska Department of Health Sponsored by:
Division of Community Health Nursing
Development Systems, Inc.,
Region VII Title X Training Office**

III. INFORMED CONSENT TO TREATMENT

A. What is consent to treatment?

1. The doctrine of consent is founded upon the legal theory of battery. The unauthorized touching of one person by another constitutes battery and can give rise to a claim for damages.
2. In a health care setting, the activity which gives rise to a battery is the unauthorized provision of care and treatment. Therefore, before care and treatment is rendered, the consent of the patient must be obtained.
3. In recent years the doctrine of consent has been modified to require that before a patient can knowingly consent, he must have sufficient information upon which to base his consent. The consent must be "informed" before it will be held to be valid.

B. FORM VERSUS PROCESS

1. Many people think of consent to treatment as a form or the document patients sign to indicate their agreement with procedures their physician believes are advisable and necessary.
2. Consent is a process, not a form. Consent is the dialogue between the patient and the health care providers in which parties exchange information and questions, resulting in the patient's agreement to a specific procedure.

C. WHY IS THERE A NEED FOR INFORMED CONSENT?

1. Assault and battery;
2. Negligence theory;

D. BASIC CRITERIA FOR A VALID CONSENT

1. Need for a voluntary, informed consent to particular procedures.
2. The patient must possess both legal and mental capacity to give consent.
3. Patients must possess sufficient information with which to reach a decision regarding treatment.

E. PATIENT'S LEGAL CAPACITY TO GIVE CONSENT

1. In the absence of a court Order, a person is presumed to be capable of giving informed consent to treatment.
2. Individuals under guardianships: Suggest that the guardian be looked to for consent to treatment.

- a. Requesting copies of the guardianship documents are important.

F. PATIENT'S MENTAL CAPACITY TO GIVE CONSENT

Patients must have the ability to understand the nature and consequences of authorizing treatment. Patients lacking mental capacity cannot give a valid consent.

1. Mental incapacity and authorization of treatment. If it has been determined that a patient lacks the mental capacity to give consent to treatment, consent must be obtained from someone authorized to act on behalf of the mentally incapacitated patient. In nonemergency situations, there may be time to request appointment of a guardian if none exists.
2. Retarded patients. (See GOARC position attached as exhibit A.)

G. CONSENT TO SPECIFIC PROCEDURES

When a patient gives consent to medical or surgical treatment, the authorization is limited to the procedure specifically discussed with the physician.

1. The consent form should be seen as an account of the consent process that took place between the patient and the health care provider, documenting each party's understanding of the agreement.
2. Ignoring specific patient instructions. If a patient gives a physician specific instructions not to perform certain procedures, ignoring such limits can lead to litigation.
 - a. Example. Patient told physician not to use a spinal anesthetic and physician agreed. During the operation, the physician used a spinal anesthesia, and the patient recovered from surgery with leg paralysis. The court found that absent express or implied consent, the surgeon had to obtain patient's consent to the anesthetic before using it.
3. Operating on a nonauthorized part of patient's body. Performing surgery on a part of a person's body different from that authorized by the patient can lead to litigation.
 - a. Example. Patient consented to exploratory surgery on her left knee. Physician operated on her right knee in error. The court held that the substitution was a technical assault, and plaintiff could recover damages.

H. VALID FORMS OF CONSENT

1. Expressed consent. When the patient in verbal or written form agrees to undergo a specific procedure.

2. Implied consent. Arises either from the surrounding facts and circumstances of a particular case or from the doctrine of Implied consent to emergency treatment. (See Section N.)

a. Example. An individual enters an immunization clinic, rolls up his sleeve, and says go ahead. This would imply he had consented to treatment.

3. Need for written as opposed to verbal consent?

a. Consent to treatment may be given verbally, and need not be written, keeping in mind that consent is a process not a document.

b. For purposes of treatment and for legal reasons, some form of documentation is necessary to record that the consent process has taken place.

I. PATIENT'S RIGHT TO REFUSE OR WITHDRAW CONSENT

1. Generally, patients have the right to refuse recommended or alternative forms of treatment and the right to forego all treatment.

2. Patients have the right to withdraw consent to treatment.

3. Patient Self-Determination Act, living will and durable powers of attorney for health care. (See Attorney General Opinion attached as Exhibit 3.)

4. Need to document patient refusal to consent to treatment.

J. ELEMENTS IN VALID INFORMED CONSENT - PATIENT MUST BE ADEQUATELY INFORMED

1. Patient must have sufficient details about a proposed procedure, including risk benefit information. If an authorization for treatment is obtained without such information, the consent is invalid.

2. The Nebraska Legislature has declared that before there may be recovery in a medical negligence case based upon the failure of a medical care provider, such as a physician, to obtain an informed consent to the treatment, the plaintiff must establish that a "reasonably prudent person in the plaintiff's position would not have undergone the treatment had he or she been properly informed and that the lack of informed consent was the proximate cause of the injury and damages claimed." § 44-2820. Informed consent is defined in § 44-2816 as "consent to a procedure based on information which would ordinarily be provided to the patient under like

circumstances by health care providers engaged in a similar practice in the locality or in similar localities.

3. Traditional standard for disclosure is measured by what is the customary practice in the medical community for physicians to disclose to patients.

a. Description of the proposed treatment in lay terms so that the patient understands the nature of what is proposed.

b. Risks of the proposed treatment.

c. Alternatives to treatment and risk of the alternatives.

d. Nebraska rule. Nebraska adheres to the "professional" theory, under which expert evidence is indispensable to establish what information would ordinarily be provided under the prevailing circumstances by physicians in the relevant and similar localities.

4. JCAHO statement on informed consent. Organizational policies and procedures describe the mechanisms by which the following rights are protected and exercised:

a. The right of the patient, in collaboration with his/her physician, to make decisions involving his/her health care, including the right of the patient to accept medical care or to refuse treatment to the extent permitted by law and to be informed of the medical consequences of such refusal;

b. The right of the patient to formulate advance directives and appoint a surrogate to make health care decisions in his/her behalf of the extent permitted by law;

c. The right of the patient to the information necessary to enable him/her to make treatment decisions that reflect his/her wishes;

d. The right of the patient to information, at the time of admission, about the hospital's patient rights policy (ies) and mechanism for the initiation, review, and when possible, resolution of the patient complaints concerning the quality of care;

e. The right of the patient or the patient's designated representative to participate in the consideration of ethical issues that arise in the care of the patient;

f. The right of the patient to be informed of any human experimentation or other research/educational projects affecting his/her care or treatment;

g. The right of the patient, within the limits of law, to personal privacy and confidentiality of information; and

h. The patient and/or the patient's legally designated representative has access to the information contained in the patient's medical record, within the limits of the law.

K. WHO SHOULD OBTAIN CONSENT?

1. Rule of thumb. The duty to disclose pertinent information rests with the caregiver who is to perform the procedure, be it diagnostic tests, medical care, or surgery.

a. Examples. In a diagnostic setting, the person carrying out the diagnostic test should obtain consent. The family practitioner may refer a patient to an ambulatory care center for a diagnostic test, but the person performing the procedure must secure the patient's consent to the procedure.

3. Dangers of delegating the disclosure responsibility.

a. The person who is given the task of obtaining consent may be able to outline broadly the procedure or test may not know much about the patient. The person may not be able to provide accurate information regarding risks and benefits for treatment options.

b. The risks associated with delegating the task of obtaining informed consent make it clear that the caregiver should personally complete the process himself or herself.

L. BASIC ELEMENTS OF A NEGLIGENT CONSENT LAWSUIT

1. What the plaintiff must prove.:

a. A patient-physician relationship existed;

b. provider had a duty to disclose certain risk information;

c. There was a failure to provide the information and the health care provider's failure cannot be excused;

d. That, had the provider furnished the patient with the undisclosed information, the patient would not have consented to treatment; and

e. The provider's failure to disclose this information was a proximate

cause of the plaintiff's injury and damages claimed.

2. Jones v. Malloy, 412 N.W.2d 837 (Neb. 1987).

M. DEFENSES TO NEGLIGENT CONSENT LITIGATION

1. Remote and commonly known risks.

a. One defense is effective for risks that are either commonly known or so remote that they do not warrant disclosure.

b. One type of commonly known risk is one that, because of a patient's past experience, he or she appreciates.

(1) Example. Patients who undergo hemodialysis twice a week do not need to be informed of the risks every time they report for treatment. However, if the format for the dialysis changes or a new procedure is introduced, patients must be told.

2. Patient acceptance of treatment regardless of risk. If a patient agrees to treatment regardless of the risks or specifically tells the health care practitioner that he does not wish to be informed, the patient cannot later bring a negligent consent action.

a. Importance of documentation if a patient accepts treatment under the above-referenced circumstances.

N. WHEN CONSENT IS NOT NECESSARY

1. Medical emergencies. Health care providers have the right to provide treatment in an emergency situation without a patient's consent.

a. Two factors must be present for the emergency exception to apply:

(1) Patient is incapacitated and cannot exercise his mental ability to reach an informed choice;

(2) A life or health threatening disease or injury that requires immediate treatment is present. The nature of the illness or injury must be such that any delay would mean certain death or serious permanent impairment.

b. Treatment which is permitted under emergency exception is limited to what is reasonable under the circumstances.

(1) Example. A procedure that is not necessary or reasonable in the context of an emergency treatment is not authorized. Performing an elective

procedure during the course of emergency care cannot fall within the emergency exception.

c. Reasoning behind the emergency care exception. Reasonable persons would rather be treated than to suffer permanent injury or death.

2. Use of therapeutic privilege. If disclosure of certain information will have an adverse effect on the patient's condition or health, the law will allow a health care provider to withhold such information or to phrase it in manner that will not upset the patient.

a. The decision to withhold information must be based on a practitioner's medical judgment and must take into account the patient's circumstances (i.e., is the patient very tense, upset, or nervous).

b. The physician must believe that full disclosure of the information will have an adverse impact on the patient. If the patient tells practitioner that he does not wish to be informed, the practitioner may proceed without obtaining informed consent.

c. Documenting the patient's wishes is very important.

3. Patient requests not to be informed.

4. Patients undergoing repetitive or continuous treatment. If patients are undergoing repetitive treatment (i.e., chemotherapy, dialysis, etc.), fully informed authorization before each course of treatment is unnecessary.

a. In the event any changes in the procedure are introduced that would change the risks, benefits, or discomfort, then a new consent is necessary.

b. Importance of asking patients if they have experienced any side effects since the last treatment, and whether they have any questions is important.

0. WOMEN AND REPRODUCTIVE MATTERS

1. Birth control and consent. A number of cases have dealt with physician's alleged failure to warn the patient about risks of using birth control medication, devices, or other drugs.

a. Example. Patient who suffered a stroke claimed that the physician

never informed her of certain risks, including blood clotting, associated with birth control pills and that the physician never gave her any literature or booklets on the subject. The court held that issues regarding informed consent should have been presented to the jury.