232229

THE WORK GROUP FOR THE COMPUTERIZATION OF BEHAVIORAL HEALTH AND HUMAN SERVICES RECORDS

4 Brattle Street, Cambridge, MA 02138 . Tel: (617) 864-6769 . Fax:(617) 492-3673 . www.workgroup.org

U.S. Department of Health and Human Services
Assistant Secretary for Planning and Development,
Attention: Privacy-P
Room G-322A,
Humphrey Building,
200 Independence Avenue, SW
Washington, DC 20201

February 17, 2000

Dear Secretary Shalala,

It is with great pride that I respectfully submit, on behalf of the Work Group for Computerization of Behavioral Health and Human Services Records, comments on your proposed privacy regulations, as they were announced in the federal register Vol. 64, No. 212, on November 3,1999 and entitled, *Standards for Privacy of Individually Identifiable Health Information.*

Before launching in to the heart of our discussion, we want to thank you and staff for meeting the deadlines and requirements of the Health Insurance Portability and Accountability Act of 1996. We share your concern about the limitations inherent to a regulations promulgated by DHHS and will do our part to urge congress to pass more comprehensive and enforceable privacy legislation, in keeping with the true initial intent of HIPAA. We recognize that you and your staff were left with a monumental task and little time to accomplish it. Now it is imperative that we do our part and provide you with a high level overview of our primary concerns and reactions to your specific requests for comment.

This document will describe: the mission of the Work Group and why it is qualified to be a voice for the fields of behavioral health and human services; our process for gathering input to and developing the attached comments; the comments themselves; and concluding recommendations.

Once again we want to commend you for your efforts and urge you to take note of our serious concerns. We are ready, willing and able to assist you with the operational issues associated with incorporating any and/or all of our recommendations in to the privacy regulations, and/or more comprehensive legislation emerging from congress over time.

Sincerely,

Dorothy Webman

Dorothy Webman DSW
Chair
The Work Group for the Computerization of Behavioral Health and Human Services Records

The Work Group

The primary mission of The Work Group for the Computerization of Behavioral Health and Human Services Records, Inc. is to create and promote equitable standards and guidelines for ownership privacy, confidentiality, quality, and accessibility of the behavioral health and human services records. In carrying out its mission, The Work Group is committed to the following: (1) to create and promote equitable standards for information access, privacy and confidentiality, including informed consent; (2) to create, monitor, and promote standards or guidelines for assessing the quality of behavioral health and human services records; (3) to promote sharing of data, consumer education; and (4) to develop a collaborative protocol for stakeholder participation.

The Work Group is a non-profit, 501(c)3 voluntary organization. It represents an alliance between members of public and private behavioral healthcare and human service systems and the family and consumer advocacy communities dedicated to ensuring that the transition to a computerized record evolves in a way that is beneficial to children, families, other consumers, providers, payors, researchers, and regulators.

The Executive Committee of The Work Group is composed of a diverse group of individuals whose jobs range from chief information officers and directors of quality management, to providers and to consumers. Leading organizations in the public and private behavioral health and human services are represented. The members of the Executive Committee have worked on projects of national scope for the U.S. Center for Mental Health Services as well as large-scale projects within their respective organizations.

Therefore, **since we are committed to advancing the use of state-of-the-art, affordable technologies toward the end of improving the quality of all health care related services, the protection of private health care information, and the well being of all people, we feel qualified to respond to this announcement.**

A Call for Equitable Regulations and Standards

Our core concerns with the proposed regulations emanate from the absence of equitable attention to concern for the health information of individuals who use behavioral health and human services. In the proposed rules you state: "In order to receive accurate and reliable diagnosis and treatment patients must provide health care professionals with accurate detailed information about their personal health, behavioral health and other aspects of their lives." The spirit of this comment is one of inclusion and comprehensiveness and one we appreciate. We respectfully request that you carry this spirit throughout the regulations. Additionally, we request that you attend to privacy rights from the perspective and vantage point of the consumer above all else.

The Work Group operates according to the following principles:

- All individuals have a right to basic health care, including behavioral health and human services.
- Any electronic database or record must include all aspects of health care including behavioral health and human services.
- All individuals have a right to privacy and confidentiality. This right must be maintained in behavioral health and human services record-keeping.
- All information in behavioral health and human services records must be treated as highly sensitive and be subject to the most stringent security systems available.

At the time when HCFA requested feedback on the data transaction standards and confidentiality, the Work Group submitted comments and delivered testimony to the NCVHS on those standards and confidentiality issues as well. The concerns we aired then continue to be relevant to this discussion. Therefore, we will highlight the final recommendations from the data transaction standards testimony here for your consideration (the full testimony can be viewed on the NCVHS website as testimony from Dr. Dorothy Webman and Dr. Jean Campbell, on confidentiality):

Please allow us to meet with you to discuss these rules and share our knowledge of the work done in this area by the behavioral health and human services industries.

1. **Please seek input from data standards, data exchange, privacy, and consumer groups from behavioral health and human services fields** (including The Work Group for Behavioral Health and Human Services Records and the Mental Health Statistics Improvement Programs Ad Hoc Advisory Committee)

2. **Please ensure behavioral health and human services parity in your approach to establishing and promulgating standards for electronic data exchange.**

3. **Please develop more detailed guidance about the technological solutions for ensuring privacy and confidentiality (such as encryption and tirewalls).**

4. **Please offer more guidance about adherence to regulations and laws governing privacy and confidentiality including training requirements and performance measurement issues guidance.** We understand that you have proposed a set of penalties for violations but you have not described processes or regulations that must be followed or developed to ensure privacy.

5. **Please develop, with the guidance of experienced persons, more detailed data sets that are specific to behavioral health and human services aspects of integrated health care systems.**

6. **Please add a family code to the data set.** The omission of this code causes the assignment of multiple case managers to one family and costs the government excessive amounts of money. Furthermore the families are overburdened and underserved by this sort of intervention.

7. **Please develop and require standards for facsimile transmission and telephonic response systems.** This guidance says that these forms of communication are not to be covered here; however our experience in behavioral health is that most agencies make the most serious violations of privacy and confidentiality via these communication vehicles.

8. **Please develop and include a means of coding social functioning and other information vital to behavioral health records in the data element prototype.**

9. **Please describe in more detail the standards for Internet and Intranet data exchange of behavioral health and human services information pertaining to the health care encounters, care coordination and claims processing.**

While some of these recommendations may seem specifically pertinent to data content, absence of attention to them has now led to the development of privacy regulations that does not cover the details involved in protecting the exchange of this type of data. Furthermore, the general absence of attention to

the subtle differences in exchanging certain types of information within covered categories, i.e. pharmacy and lab information, has also led to privacy regulations that are not sensitive to the unique issues of behavioral health and human services consumers. We therefore, urge you to work with NCVHS to extend the scope of covered information and end users to include all those in need of a full range of health related services, including behavioral health and human services.

Our Process for Gathering Input about the Proposed Privacy Regulations

On Dec 12, 1999 a sub committee of the Work Group convened in Washington, D.C. We invited colleagues from other stakeholder groups to participate in the meeting including but not limited to: the American Managed Behavioral Health Association; the Federation of Families for Children's Mental Health; The National Mental Health Association; the National Association of State Mental Health Program Directors; several county health department leaders; the National Alliance for the Mentally Ill; other consumer advocates; and representatives of the Mental Health Statistics Improvement Program. Few were able to attend due to the short notice. Due to the voluntary nature of this effort, the majority of the consensus building took place at this time. However, we plan to circulate this document after submission to get endorsement from other stakeholders. We will forward additional letters of support as they arrive.

At a later date, two Work Group members submitted more detailed input in the areas of technological solutions for privacy protection and consumer concerns with the proposed regulations. A full list of the Work Group members is provided as an attachment to this document. In addition to Work Group members, Trina Osher of the Federation of Families for Children's Mental Health, Dr. David Bearman of the Santa Barbara Regional Health Authority contributed to the text of this document.

Since the regulations came out at holiday time and the behavioral heath industry does not have an organized infrastructure as the health care industry has around data and transaction standards, it was difficult to mount this effort It is, in fact, part of our recommendations that DHHS consider extending additional financial support to the voluntary standards groups, such as the Work Group and MHSIP, which have emerged in the behavioral health arena. These groups have developed some of the data content and guidance that could be used to flesh out the proposed regulations. We believe they can provide significant assistance in the implementation of the administrative simplification data sets and accompanying regulations. They will require additional support, however, to complete the job and provide you with useful information. We urge you to contact Dr. Ronald Manderscheid of SAMHSA for more information about these groups.

We believed, going into our meeting to review the proposed regulations, that we would have only the one-day. At the end of that day, we got news of the extension for comment. We were able to mount some additional volunteer help after the meeting, but again, absence of advanced notice hindered our ability to muster additional assistance.

Thus due to time limitations and lack of paid staff we had to pick and choose priority areas for comment. We divided ourselves into three groups and each group reviewed a different section of the regulations or covered a topic related to it. The groups prioritized and selected their top three issues for comment. We added additional groups to focus on technological and consumer perspectives of the regulations. The attached comments reflect our collective efforts.

Please be advised that our group would be happy to serve you by providing additional guidance and support if you request this help and can convene a meeting to facilitate this knowledge exchange.

Setting a Context: Our Perspective of the Issues

It is our belief that most participants in the behavioral health and human services fields are relatively unaware of HIPAA and the implication of the Administrative Simplification Act on their work. This is, in part, due to the emphasis in the Act on physical health information and a misunderstanding of the scope of the covered end users. As a result, behavioral health and human services professionals have not believed this Act will effect them.

Given that implementation of this Act will effect their work, we implore you to incorporate into the language of the proposed rule attention to the need to fully educate all stakeholders, including providers and consumers of allied health, human services and behavioral health services, about the requirements of the Act. We believe it is with in your purview and that of ASPE to *require* education of these sub-sectors.

The White House Conference on Mental Health; the Surgeon General's report; Mental Health Statistics 1998 and other forms of federal guidance have marked the simple and grave need to meet the comprehensive health needs of residents in the U.S., including their behavioral health and human services needs. The Administrative Simplification Act is intended to create efficiencies in our health care delivery systems and enable us to gather data needed to determine best practices. Given that best practices can only be determined via a comprehensive understanding of all of the intervening variables affecting one's health it is imperative that the privacy rights of all individuals, including those recipients of behavioral health and human services be delineated within these regulations.

Members of our community have made repeated efforts (via testimony to NCHVS) to educate decision-makers about the need for behavioral health and human services parity within HIPAA and the Administrative Simplification Act, with minimal success.

We believe that perhaps one of the biggest and most egregious errors made with the HIPAA itself, separate and apart for the privacy regulations, was the inadequate attention to the overlap of health information within other behavioral health human services record keeping systems. Due to this oversight, its proposed implementation milestones articulate a business model for this nation's health care system that is not coordinated, not comprehensive, and not responsive to consumer needs. **It leaves out core pieces of their health related needs, including behavioral health and human supports. This seems to have reduced the scope of the data exchange protocols and the privacy regulations to a technology plan that is mapped to an inadequate business model; one that places the needs of the consumer to control his/her health information in last place. We urge you to move consumer concerns to the forefront of your agenda by incorporating mechanisms for consumers to read, write on and access their records at any moment in time. We also respectfully request that you include more far-reaching recommendations for consumer education about their privacy rights. Furthermore, we implore you to mandate informed consent standards for every transaction of individually identifiable information. This is possible to do with a keystroke today. This will not place any undue burden on the provider or consumer and it will increase consumer confidence and participation in their own health maintenance.**

We firmly believe that it is necessary to ensure privacy via both technological and legal or regulatory solutions. **The proposed privacy regulations should incorporate additional attention to potential technological solutions for securing the record and at a minimum more heavily reference the new HCFA guidelines for use of the Internet to exchange health related information.**

We also believe that technology plans should mirror good business models. Most of our comments are rooted in our dire concerns about the absence of attention to that comprehensive business model. We believe you have done the best you could to build guidelines to mirror the business model you were forced to work within; not the one that would truly create efficiencies among and between the multitudes of service delivery systems for which you have oversight responsibility. Our comments reflect different perspective of service delivery systems and their business models as well as the privacy issues inherent to stakeholders in those systems. We believe in parity and the full integration of behavioral health and human services. In this day and age virtual integration is more likely than full services integration; making the guidelines in the Administrative Simplification Act all the more potentially powerful.

To that end, we urge you to adopt a more comprehensive approach to these privacy regulations; extending them to at least all departments and divisions of DHHS.

SPECIFIC COMMENTS ON THE PROPOSED RULE

I. Background

A. The Need for Privacy Standards"

There clearly is a need for privacy standards. As we stated in our cover letter, we want to thank you and staff for meeting the deadlines and requirements of the Health Insurance Portability and Accountability Act of 1996. We share your concern about the limitations inherent to a regulation promulgated by DHHS and will do our part to urge congress to pass more comprehensive and enforceable privacy legislation, in keeping with the true initial intent of HIPAA.

In the proposed rules you state: "In order to receive accurate and reliable diagnosis and treatment patients must provide health care professionals with accurate detailed information about their personal health, behavioral health and other aspects of their lives." The spirit of this comment is one of inclusion and comprehensiveness and one we appreciate. We respectfully request that you carry this spirit throughout the regulations. Additionally, we request that you attend to privacy rights from the perspective and vantage point of the consumer above all else.

Please develop more detailed guidance about the technological solutions for ensuring privacy and confidentiality (such as encryption and firewalls).

We urge you to move consumer concerns to the forefront of your agenda by incorporating mechanisms for consumers to read, write on and access their records at any moment in time. We also respectfully request that you include more far-reaching recommendations for consumer education about their privacy rights. Furthermore, we implore you to instate informed consent standards for every transaction of individually identifiable information. This is possible to do with a keystroke today. This will not place any undo burden on the provider or consumer and it will increase consumer confidence and participation in their own health maintenance.

In the background section, the Proposed Rule asserts "The expanded use of electronic information has had clear benefits for patients and the healthcare system as a whole." To date there has been no systematic study of the actual benefits and harm of this development. Certainly there have been benefits to the health care providers and this proposed law paves the way for the rapid

expansion of access to electronic health records by health providers and third parties. However, in fact, there has been considerable anecdotal information as to both benefit and harm. Further, the proposed rule claims that use of electronic information has helped to improve the quality of care delivered in the U.S. This remark is also unproven and any statements that claim the value of electronic information systems must do this with great care and acknowledge the lack of proof for this contention. Yes, it could have both benefits and improve the quality of health care but this is a promise that is contingent on the development of other social forces such as the growth and empowerment of health consumers-particularly their ability to access, understand, and provide feedback regarding health information-and the implementation in both the spirit and the law of the proposed rule under consideration. We question whether the use of these standards will "most clearly benefit patients" as stated in the proposed rule without more attention paid to the real concerns of health consumers for protections that go beyond what is currently proposed. The flawed but pervasive assumption of HHS that electronic access by the health providers and third parties is both a public good and inevitable must be addressed in order to begin to move towards support of protections and rights not deemed practical in the proposed law. In order to truly understand the perspective of the health consumer as this proposed law claims to appreciate, we recommend that you review the chapter in the book *Privacy and Confidentiality in Mental Health* Care by Dr. Jean Campbell entitled "Consumers' Perspective of Confidentiality and Health Records" which is enclosed in the appendices of these comments.

Ultimately Americans want to be genuinely protected and their individual medical privacy enhanced through the enforcement of long established privacy principles based on constitutional and statutory law, common law, the Hippocratic oath, the canons of medical ethics, and common sense.

B. Statutory Background

Relationship to State Laws (160.202)
We strongly urge the Administration to maintain the requirements that these federal rules supersede weaker state laws, but that they not preempt more privacy-protective state laws.

However, we are concerned about the provisions that permit states to receive a waiver of these standards on the grounds that a weaker state law is needed to improve program efficiency or effectiveness. If states are allowed to retain their weak privacy laws too easily, citizens in these states would not benefit from the federal rules. We oppose such a waiver. If there is to be a waiver for such purposes, however, then at the very least the process must be open for public participation. Members of the public, health care providers and other interested parties should be able to submit their comments on a state's request to retain weak privacy laws. HHS should consider these comments in making its decision whether to grant the waiver, and should also consider the impact of the waiver on quality of care or access to care.

Section 160.203(a)(1)(iv) and(d) should be deleted

The carve out for public health is tine as long as it is not used as a loop hole to gain access to otherwise protected information. Section I definitions does help define what type of state laws to be preempted are contemplated.

The issue of how to propose culture would operate relative to specific state laws is very important. Clearly it requires review by people in your group familiar with security privacy laws in the state and whether or not they provide more protection than the proposed regulation.

C. Consultations

The proposed rule states that The Congress explicitly required the Secretary to consult with specified groups in developing the standards under sections 262 and 264. Section 264(d) of HIPAA specifically requires the Secretary to consult with the National Committee on Vital and Health Statistics (NCVHS) and the Attorney General in carrying out her responsibilities under the section. You also describe the groups you did engage in the key informant process. We were proud to be included in some phases of this process. Yet we are concerned that the voice of behavioral heath and human services has not yet been incorporated into these regulations as fully as we would like and that the behavioral health standards consumer groups have not been as actively involved in the process as they could be. **Please develop, with the guidance of experienced persons, more detailed privacy regulations and data sets that arc specific to behavioral health and human services aspects of integrated health care systems.**

D. Administrative Costs

No comment

E. Summary and Purpose of Proposed Rule And II. Provisions of Proposed Rule

We found that many of the issues we found with the proposed rule were embedded within the context of the provisions therefore we have consolidated our comments for these sections into one unit.

We want to be perfectly clear that we fully support extending this regulation, and hopefully more comprehensive legislation, to other areas of DHHS and paper records, facsimile transmission and all transactions of health, behavioral health and human services information

Children And Adolescents Sec. 160.202

We support the wording of the regulation as it stands. We agree that adolescents and certain other youth deserve protection from the disclosure of some specific health care information to parents, but there needs to be uniformity of regulations among states. We would propose federal regulations governing disclosure of certain information about minors to parents, in order to gain uniformity of regulation and protection.

On the other hand, when this information is not disclosed to parents, there should be immunity from suit on the basis of the information withheld from parents.

This entire area needs study on a national level

Definitions (160.504)

Individual

The Preamble stipulates that when an individual is legally incapacitated, others making health care decisions for the individual may access the individual's records specifically, that a person informally designated as the patient's health care decision-maker may access the record. However, the language in the proposed rule itself refers only to those who have been given power of attorney and omits reference to informal decision-makers, health care agents or health care proxies appointed through an advance directive. Section 164.504 of the rule should be amended

to include individuals acting as health care agents or health care proxies under the terms of an advance health care directive in the definition of "Individual" (paragraph (l)(i)).

Protected Health Information

The proposed rule excludes from protection all identifiable health information of inmates of correctional facilities and detainees in detention facilities, including individuals who have been released. Many individuals with serious mental illness come in contact with criminal justice authorities as a result of behaviors stemming directly from their illness; these provisions will cause serious problems for them. Furthermore, many inmates also suffer from ATOD addictions ;these provisions will cause serious problems for them too.

The rule is too sweeping in its exclusion of jails and prisons from its privacy protections. Access without consent may be acceptable for some purposes but it is not universally acceptable. For example, it is appropriate to share health care information with other medical facilities when the inmate is transferred for treatment. There can also be reasons not to share information with the individual in the cases cited in the Preamble regarding transfers and other specific correctional facility activities.

However, blanket authorizations for fishing expeditions by jail personnel at the time of arrest and prior to conviction are not appropriate. Individuals have the right to privacy concerning their medical records and the right not to identify themselves as having a mental illness, particularly if they believe this will put them at risk (from other inmates or from discriminatory actions by jailers) while in a detention facility. In order to treat mental illnesses in jail, correctional officials could screen for mental illness but they should then seek authorization to access appropriate records for individuals who wish to be treated in jail. Individuals who are not a danger to themselves or others have the right to refuse treatment and to refuse access to their private medical records.

In addition, jails and prisons should not share private medical information of discharged individuals. This may seriously impair an individual's rehabilitation into society. Disclosing the fact that an individual was treated for mental illness while in jail could result in significant further discrimination against the person in attempts to reestablish him/herself in the community.

This definition should be amended to delete the exception for jails and prisons and to substitute language allowing certain information in certain specific situations to be considered unprotected health information (as per discussion above).

Treatment

The definition of treatment includes case management and disease management programs. There are many forms of disease management, but some can result in the sharing of information in ways that are not privacy-protective (such as leaving messages on an answering machine that a psychotropic medication prescription has been renewed). Specific protections are needed against certain aspects of disease management, at least for highly sensitive areas.

Appropriate sections should be amended to require plans to ensure that case management and disease management are conducted in a manner fully protective of individual medical privacy and to require plans to take steps to ensure that unauthorized individuals will not, as a result of such a program, be given access to protected health care information.

Sec. 164.504, (e)(ii)

We agree with the sentiment, but it needs rewording for clarification

164.506(a) "General Rules: Treatment, Payment and Health Care Operations"

We oppose the provision that a covered entity be permitted to use or disclose protected health information without individual authorization for treatment, payment, or health care operations. We question the assumption that requiring authorization would be unrealistic in an increasingly integrated health care system, but we point to the rapid advance of information storage and retrieval systems that could allow for new technological methods to ease the time and burden for gaining authorization. The requirement for separate authorization would not necessarily delay and impair care if methods to gain authorization were encouraged to develop. Allowing wide access without authorization in the treatment, payment and health care operations could certainly cause substantial harm to individuals and undermine the entire effort to enhance privacy protections for individuals.

What is particularly troubling is the inclusion in this exemption of internal quality oversight review and outcome performance of providers participating in their network when authorization would be relatively easy to obtain. These quality oversight functions have not proven to this date to greatly enhance the quality of health care delivery. In fact, protecting the rights of individuals to access to such reports which is not guaranteed by this proposed act may be a more reliable way of insuring health quality.

We are also concerned that covered entities could make disclosures to non-covered entities for payment purposes and the proposed rule to protect confidentiality ends. Certainly health consumers should be notified if such a transfer is made as a minimum protection to the individual. Then the individual could monitor the frequency of such disclosures, the protections of the non-covered entity, and could decide if they would withdraw consent for use of their records in this manner. Even more desirable, would be the requirement that under no conditions should such data be transferred to non-covered entities with authorization of the health consumer.

Comments On "Uses And Disclosures With Individual Authorities"

WARNING: We believe that the potential abuses of the regulations governed in this section present potentially serious conflict of laws, and erosion of privacy and individual rights.

Permitted uses include, "Disclosures and uses for judicial and administrative proceedings"--(W)

This section is worded too broadly and conflicts with statute, case law, and published ethical guidelines of various organizations and professions. This section should be much more strictly worded to protect the privacy and established evidentiary privileges. Additionally, due process rights need to be afforded. Finally, under subsection (i) the order must be a lawful one issued by a court and subject to jurisdiction with notice to the individual.

Exceptions Introduction to Uses and Disclosures without Individual Authorization

Generally, disclosure without authorization needs to be limited to the most extreme circumstances. Further it must recognize existing protections that relate to privacy, privilege and confidentiality. This section appears to be trying to supersede much existing law that better protects the rights of the individual.

Law Enforcement

In terms of disclosure to law enforcement, law enforcement should be required to obtain a court order with notice to the individual for the disclosure of covered information. Prior to ordering the release of such information, the court should review the record *in* camera to determine its relevance and balance the individual's right to privacy and due process against the law enforcement agency's need to know.

There should be specific civil and criminal penalties for ***unauthorized release of medical, substance abuse, psychiatric, or other health core information that results in:***

1. ***Denial of employment***
2. ***Discrimination in the provision of health care***
3. ***Discrimination in housing***

(c) We propose that it be clearer that these investigations be specific to the health care system, not to include other possible criminal or civil actions.

(f)(C) This section is not acceptable in that it appears to supersede areas of criminal law, rules of evidence and civil procedure. This section needs to be rewritten in consultation with the bar.

(2) Release of "Limited information for identifying purposes" should be much more broadly protected. Can police, for example, release information that a celebrity is in a substance abuse treatment program without fear of sanction?

Law Enforcement - a consumer perspective

The proposed rule, while it creates the illusion of legal barriers before records may be provided to law enforcement, establishes no meaningful legal process. Law enforcement agents may issue written demands that will require doctors, hospitals and insurance companies to provide individual, identifiable health care records. Although the written demand must assert the relevance and narrowness of the request, there is no requirement for judicial review of those assertions and no mechanism for the individual to contest this disclosure.

Another provision in the rule allows release of patient information whenever the police are trying to identify a suspect. This would allow all computerized medical records to be used by the police as a database, through which they may browse at will to seek matches for blood, DNA or other personally identifiable health traits. Substantial revisions are needed to this section of the rule. In all instances, a judicial procedure should be required before law enforcement officials can access identifiable medical records.

- **Minimum Necessary Use and Disclosure (164.506(h))**

  Limiting disclosure of information to only that required to accomplish the intended purpose should not be qualified by taking into account "practical and technological limitations." It may be quite difficult or more expensive to limit access to the full medical record, or to portions thereof. However, for certain highly sensitive areas of health care, higher levels of protection need to be in place. It is not necessary, for example, for a physician treating an individual for a foot problem to know that the individual has been in psychotherapy.

  Health plans should "consider" the need to have higher protections for certain very sensitive areas of medical information, such as mental health or sexually transmitted diseases. It is extremely important that providers and plans give consideration to the fact that certain highly sensitive information requires exceptionally high standards of confidentiality. Section 164.506(b) should be amended to require health care organizations to consider whether unique authorization requirements should be established for highly sensitive information, including information about HIV/AIDS and other sexually transmitted diseases, reproductive health, genetic information, abuse and neglect, drug and alcohol abuse and mental health.

- **Right to Restrict (164.506(c))**

  While we strongly endorse the language in the proposed rule granting individuals the opportunity to request additional privacy protections from their health care provider or plan, this needed protection as determined by the health consumer is dependent upon cooperation from the provider or plan.

  Therefore, it will only allow certain individuals in particular situations to secure desired protections for their individual health records. Without receiving the desired protections, including an informed consent protocol, an individual is forced to chose between receipt of services and waiver of rights, For example, health consumers should not be forced to give insurers blanket access to medical information in exchange for health coverage. There is no place in this proposed act that would allow consumers to "opt out" of an electronic record system (i.e., the organization would keep a person's health records in paper form with some limited exceptions). Researchers have argued that incomplete data and therefore bias would then be introduced into outcome studies if this option were provided. However, this claim is not based on any field research that would determine how many consumers would opt out, or whether the number would be constant, based on respondent bias, or reflective of organizational policies that would cause consumers to mistrust the protections in the electronic information system. If the consumer believes that the benefits for inclusion outweigh the dangers, and if the consumer trusts the organization to keep medical records secure, then few would take the option to stay out of the electronic information system. To leave it up to the provider to decide whether protections desired by consumers are acceptable undermines the principle of "informed consent" and introduces coercion into the process.

  It is also important that this provision include the right of individuals who are paying directly for their care to request that there be no sharing of their health care information. Many persons pay out-of-pocket for mental health services for this very reason, and should continue to be able to do so.

There needs to be specific, severe civil and criminal penalties for:

a. Inappropriate disclosure of covered information
b. Coercive methods of obtaining authorization

The information released in these records must be much more strictly regulated. It must not include, for example, data about biological fluids, such as genotype or genetic risk data; EEG; EKG; neuroradiologic data; and other similar test data. This includes test data not normally part of an administrative health record. These data must clearly be regulated by other rules.

There also needs to be a private right of action in order to enforce these privacy and confidentiality regulations.

These regulations create a less stringent standard for health care information for children and adolescents than is covered by the Family Educational Right and Privacy Act (FERPA). We suggest that where there are several levels of confidentiality protection, that the stricter levels of protection apply (e.g. these regulations vs. FERPA).

******Advanced Directives*********

There should be provisions for Advanced Directives, so the individual can designate those who have access to his health care records. These provisions should protect the health care records of the individual from unauthorized access.

********Over-riding these protections**********

In the event of a national or regional health care emergency, there should be a provision allowing for a Presidential declaration to suspend these regulations, This declaration should include a complete scope of the suspension, and a date specifying its termination.

These regulations should be extended to include all persons within the contiguous United States, including foreign nationals and illegal immigrants.

Uses and Disclosures for Which Individual Authorization is Required(164.508)

- **Employer Access**

Additional protections are needed to prevent harmful employer access to employees' medical records.

Supervisors should not have access to this information. It is particularly important to extend the scope of the regulations' protections to all employers and to cover workers' compensation records. The Administration is urged to develop legislative recommendations for Congress in this area, since the scope of its authority is too limited to deal with the issue appropriately.

- **Individual Authorization (164.508(a)(2))**

We strongly support the part of the rule that requires specific individual authorization before personally identified health care information may be used or disclosed for purposes other than treatment, payment, health care operations and certain limited other circumstances, such as public health and research. In particular, it is extremely important to require specific authorization

before this information is used for purposes of marketing or commercial gain or fund-raising. However, there is significant commercial gain from use of health records to leverage coverage, determine cost-effective procedures, market services based on satisfaction and other studies, and to even profit from both the sale of outcome management systems and outcome data that benchmarks performance. Consumers rightly feel that their health care experiences are really viewed as raw data that can be mined, processed, and sold by entrepreneurs, corporations, and academia without much concern for the welfare of the individual. In fact, it is rare when consumers are reimbursed for the burden of answering hours of questions for quality management or outcomes research.

Therefore, while this proposed rule appears to protect consumers from commercial exploitation, it ignores some of the most profitable uses of health information. For this reason, among others, informed consent should be required for such research and information control and monitoring activities.

- **Consent for Treatment, Payment and Health Care Operations (164.508(a)(2)(i)(A)**

Individuals should retain the ability to consent to who will see their medical records. Under the proposed rule, individual consent is not required for purposes of treatment, payment or "health care operations." As a result, consent would not need to be given for medical records to be used and disclosed for a broad array of purposes. Consent for the use and disclosure of records is almost always required today, so the proposed rule represents a significant change.

At the core of privacy protection that health consumers want is informed consent to control the use of their records, They want the sharing of health information to be voluntary. Some have even recommended that those groups of people, who risk great personal harm if their health information is revealed, should not have their records included in any system of electronic records.

Without specific informed consent, it is imperative that clinical records should not be retrospectively integrated into an electronic information system as currently occurs. While it is correct that current authorizations are coerced, in the sense that an individual must provide consent before being accepted into treatment, it is wrong and should be remedied by this proposed act, not accepted as standard practice. An important principle is violated if this consent is not requested, and to avoid coercion, the proposed law should provide the "opt out" choice for consumers. Then the regulations would establish a clear right to privacy and would provide that the individual has the right to control his or her medical record information.

Also, signing an authorization helps consumers to understand their privacy right and to consider privacy issues, Since the rule requires a notice of privacy practices, it would be a relatively simple matter to require that individuals be required to sign the notice so as to indicate their consent.

Section 164.508(a)(2)(i)(A) and (a)(2)(iv) should be amended to require formal, signed consent for the sharing of medical records information for purposes of treatment, payment and health care operations.

- **Exception for Psychotherapy Notes (164.508((3))**

We support limiting access to psychotherapy notes without specific consent from the individual, but the rule should make clear that it is the information contained in psychotherapy notes that is being protected, not merely the "notes" themselves. The protection for psychotherapy notes will not be meaningful if health plans can demand the same information in a different format.

Section 164.508(a)((3)(i)(A) should be amended to make it clear that the information described in the rule as being appropriate for inclusion in psychotherapy notes may not be disclosed, either by sharing the notes or by transmitting the same information in another format.

- **Additional Categories of Disclosures (164.510)**

The Preamble requests comment on whether additional categories of disclosures are permitted under proposed 164.5 10 for which the disclosure of psychotherapy notes (and the information therein) without specific individual authorization would be appropriate.

The limitations on access to psychotherapy notes should be extended to public health, oversight, next of kin and judicial and law enforcement. There is no good rationale for these notes (or the information therein) to be shared for any purpose, unless the individual so desires. These represent the personal notes of the provider concerning extremely sensitive information. The essential medical information on the individual is included in the medical record. If individuals are aware that such information can be shared so widely, it will likely destroy the therapeutic relationship.

- **Public Health (164.510(b))**

As stated above, psychotherapy notes (or the information therein) should not be released for public health purposes.

- **Judicial and Administrative Proceedings (164.510(d))**

The regulations provide no meaningful privacy protections for civil litigants. No judicial review is necessary before one party to litigation subpoenas the other party's medical records based on an assertion that the adverse party's medical condition or history is at issue in the litigation. No notice need be given to the individual before disclosure occurs. As in the law enforcement context, see below, judicial review and notice to the party whose records are at issue are essential to protect privacy. As stated above, psychotherapy notes (or the information therein) should not be released for judicial and administrative proceedings.

- **Governmental Health Data Systems (164.510(g))**

There is a broad exception in the regulations that permits health care providers to disclose medical records to government agencies or private entities acting on behalf of agencies, for inclusion in a government health data system. While such systems may initially be established to support "policy, planning, regulatory or management functions authorized by law," as the regulations state, government data are notoriously susceptible to expansion and abuse. For

example, there is an eagerness by those in politics to reveal personal health information to gain advantage, and instances in which privacy protections have been put aside in the service of public policy are not new. This proposed act might well allow federal and state agencies the very type of access that once was gained only through covert activities.

Under these regulations, consumers faced with the realization that government agencies have access to their entire medical history will engage in the same privacy protection behaviors (e.g., not seeking treatment) that give rise to the need for regulations in the first place. Therefore, section 164.510(g) should be amended to narrow the access without consent for purposes of government data systems; individuals should be provided specific information on such uses and should be able to grant or deny consent.

- Research **(164.510(j))**

We strongly endorse the extension of the common rule to privately-funded research, which will provide the same measure of privacy protection for individuals participating in private research as is now required for government-sponsored research.

If outcome studies and other services' research activities were required to have the same human subject protections as other forms of research, then individual benefit, not public benefit, would have to be weighed by the consumer against potential risks of data collection in an informed consent protocol. It is for this reason that we strongly urge the proposed act to support the requirement of covered entities to have an IRB or privacy board review their administrative procedures for both research and evaluation or quality control monitoring through data records. This requirement would not necessarily hinder these activities (except where privacy protections are not provided), but make them more responsive to the needs of health consumers for privacy. Further, with IRB oversight shared by community membership, especially by members of stigmatized or underrepresented groups, the interests of a data review panel would be broadened and become responsive to the health privacy needs of individual consumers rather than health organizations and research institutions.

A consumer researcher perspective

However. we question the reasons for exempting outcomes research and other forms of quality review from gaining consent to use health data. Probably the most disturbing claim to override consumers rights to confidentiality is the need for outcome studies. Such studies not only involve the use of records without consent, but may also require recipients to fill out intrusive questionnaires as a condition of their treatment. Consumers question the value of this type of research or performance monitoring. We wonder whether system values-in this instance, the claim of researchers to be able to lower costs and identify more effective treatments-trump the value of respect for individual autonomy. In response to Nazi atrocities in the conduct of human experimentation, the Nuremberg Code proclaimed as its first principle that "the voluntary consent of the human subject is absolutely essential." A person should be able to exercise free choice without intervention of any element of force or coercion in the use of medical information gathered through access to electronic patient records.

Rights and Procedures for Access for Inspection and Copying (164.514)

. Disclosures Reasonably Likely to Endanger Life or Physical Safety (164.514(b)

We do not support the provision allowing plans and providers to deny requests for inspection or copying of a person's own record only if the inspection or copying endangers the life or physical safety of any person when the person requesting access is the health consumer. It is hard to conceive of situations where receipt of individual health information by that individual would create a life-threatening situation.

Further, this exemption appears to undermine the voluntary participation in an electronic information system and consent protections advocated for in other portions of these comments. While we commend the Administration for granting individuals with mental illness the same right of access as other individuals, the proposed rule currently permits any health care professional to deny a person access to his or her own record. We strongly oppose this approach since mental health professionals readily and easily use the "mental illness" of the individual as a reason to deny access. Therefore, much that is both incorrect and stigmatizing continues to appear in the records of psychiatric patients supported only by the subjective impressions of the provider. If the act is to be truly responsive to individuals to access their own health data and an important means to correct abuse and misinformation, why would the proposed act rely on the medical community to prohibit individual access?

We also oppose the proposed act's decision to encourage covered plans and providers to institute a system of appeal related to denial of inspection and access, but its unwillingness to require it by regulation. Without regulation, it is hard to imagine that covered entities will voluntarily oblige denied consumers with a mechanism for overturning such decisions. Further, an exhaustive accounting of all uses and disclosures to individuals upon request seems not to really be burdensome with the capabilities of electronic information systems to collect and report such information. How would health consumers be able to judge the appropriate use of their protected health information without such an itemized disclosure?

Notes On Administrative Burden

Privacy Official 164. 518(a)

The person designated to be responsible should be high enough in the management to wield appropriate influence. Also, the person designated should meet some minimal standard (such as attendance at private, government, or state training) within a certain time frame of the regulations taking effect (12-l 8 months, for example). There also should be a C.E. requirement (4-8 hrs/year).

Training 164.518(b)

Staff turnover is fairly rapid. Therefore, two four-hour live presentations or a review online taking approximately 2 hours/year seems more practical and effective. Low level staff where turnover is highest may have a greater potential for unauthorized disclosure.

Safeguards 164.518 (c)

This section is fairly vague. There needs to be some threshold for technical and physical standards that must be met. Also may want to make some mention of routine review of these 3 areas of safeguard.

Verification 164.518 (c)

Some find of PKI credentialing certificate should be required

Whistleblower pg 59990

While somewhat difficult to prevent, malicious disclosure would apply a reasonable person rule that fraud may have been committed. Limiting the amount of information would require even more of a judgment call. One last comment is that this would not include possible criminal behavior by to patient.

Internal complaint process 164.518 (d)

The intelligence community has abused access to information before. To give them an exclusion repeating access to sensitive information just invites abuse. The unfortunate plunder in the Nixon administration and the Ellsberg affair, attempting to break into Dr. Fielding's office and to other psychiatric records, is an apt reminder that even those at the highest level of government are willing to abuse citizen's mental health privacy. Do believe that response to inquiry should be substantive and timely (e.g., within 60 days. May wish to consider some kind of arbitration)

Sanctions 164.518e

No comment. Except we would wholeheartedly concur that the severity of the sanction be proportional to the type of privacy breach and damage or potential damage to individuals.

Duty to Mitigate – 164.518 (f)

No comment.

Policies and Procedures 164.520

An accurate recording of who accessed a person's tile should be a mandated policy. It would likely be very helpful to have a privacy board for review and recommendation, but at this point, approval would give such a board too much power. Recommendation allows more flexibility to the affected entities, but with this assurance of privacy for our litigious society, a review board's recommendation would carry considerable weight.

TECHNOLOGICAL SOLUTIONS NEEDED TO SUPPORT TRUE PRIVACY PROTECTIONS

The proposed regulations reference a written consent to release information. There is no mention in the proposed regulations of how the written consent and the electronic transfer of data will be coordinated. Without a mechanism that incorporates the consent into the electronic tile, there is always the risk that information will be released electronically when the written consent is absent, expired or revoked by the patient. The proposed regulations should include a requirement to include information about the consent in the electronic file. The information should include who is providing consent (patient, family, surrogate), the date of the consent, the expiration date of the consent and the type of data to be released. By automating the content of the written consent, electronic notification would be possible when the

consent was due to expire. By including this information in the electronic file, the chance of releasing unauthorized information would be lessened.

The proposed regulations should require all entities that transmit data electronically to maintain computerized logs of the data transmittal including the date, time and destination of the data. Data should only be transmitted from one individual to another individual. This will provide for accurate audits and accountability. Each organization should be required to also maintain electronic logs of access to the data internally by their employees or contractors. Confidentiality statements should be signed by all entities that will have access to the data, whether the access is internal or external. An organization should be required to not only provide training to its employees on confidentiality and privacy, but also provide the same training to any intended recipient of the data.

The unique individual identification number should not be the Social Security Number. The Workgroup is opposed to the use of the Social Security Number as a unique identifier. Due to the highly confidential nature of health data, the use of such a common identifier would undoubtedly lead to unauthorized access to an individual's health data. Of even more concern would be the capacity to link an individual's health data with other personal data that also uses their Social Security Number as an identifier. Individuals could face denial of health care coverage or employment if their health data is indiscriminately disseminated. The media has repeatedly reported on the ease with which an individual's most personal information can be accessed, often by linking the name and Social Security Number. The research community should be tasked with developing a new unique identifier in concert with the standards groups and other interested parties. The unique identifier should be constructed in such a way that prevents its being linked to any other electronic data about an individual. Then even if it is compromised, other personal data about an individual could not be linked to their health data.

The proposed regulations do not address who owns the health data that is to be shared. Does the individual own his/her health data or does it belong to the entity that is maintaining it? Is the content of the health record owned by the individual? The World Health Organization has long proposed that the individual is the owner of their health data irrespective of the media on which it is stored.

CONCLUDING RECOMMENDATIONS AND CONCLUDING COMMENTS

1. Please know that we will do all we can to encourage congress to pass comprehensive privacy legislation.

2. Please know that we stand prepared to assist you by convening our colleagues from voluntary standards groups to more thoroughly address the privacy issues of persons who receive behavioral health and human services. In this same vain we encourage you to extend the purview of these rules to all of DHHS agencies.

3. Please consider all of the recommendations we have made to ensure direct consumer protections under these regulations The current proposed rule is not adequate for any consumer; and is extremely inappropriate for consumers with sensitive information in their heath records

4. Please pay careful attention to the recommendations we made which question the legal validity of several of the rules with regard to disclosure

5. Please hear that we do not advocate for the use of patient data without fully informed consent at each disclosure We believe consumer education about the use of de-identified data for the purposes of research will go a long way to engaging consumers in this process in a respectful a manner.

6. We strongly encourage you to add specific guidelines to this regulation about technological tools and resources that can be applied to securing the health record.

7. There must be rules preventing the resale of consumer data without explicit warnings to the consumer of the risks of allowing this disclosure.

8. We support and specifically request that you extend these rules to paper and any health record, even anecdotal verbal exchanges.

9. We encourage you and congress to fund and require training and penalty reinforcements. We are extremely concerned that the absence of funding for these proposed requirements and the monitoring of compliance or failure to comply will render the regulations meaningless.

IO. Please understand that our comments come in the context of a strong desire to bring the behavioral health field on par with the that of the health care industry in terms of data and transaction a standards as well as privacy rules. We request your assistance in notifying ASPE, HCFA, NCVHS of our interest in partnering with you to mediate these divides on behalf of al consumers of behavioral health and human services information in this country.

Thomas **Pavkov**
Assistant Professor of Psychology, Purdue University Calumet:
Head Start XXI Resource Ctr.
2200 169th Street
Hammond, IN 46323-2094
(219) 989-2029
tpavkov@nwi.calumet.purdue.edu

Robert **Shomer**
President/C.E.O., Hawthorne Community Medical Group
8550 Balboa Blvd
Northridge, CA 91325
(818) 609-1761
drshomer@eyewitnessid.com

Ivan Walks
Washington, D.C. Dept. of Health
825 N. Capitol St., NE
Washington, DC 20002
(202) 442-5999
iwalks@dchealth.com

Privacy and Confidentiality in Mental Health Care

edited by

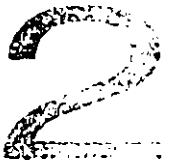
John J. Gates, Ph.D.
The Carter Center Mental Health Program
Atlanta, Georgia

ond

Bernard S. Arons, M.D.
The Center for Menial Health Services
Rockville, Maryland

PAUL H. BROOKES PUBLISHING Co

Baltimore • London • Toronto • Sydney



Consumers' Perspective of Confidentiality and Health Records

Jean Campbell

The United States has been propelled irretrievably into an era of computers and electronic networks. With this technology has come the ability and the desire to employ it in the health care field by developing databases of medical records. Electronic linkage of medical records promises improved care, both at the system level and at the individual level of service utilization. However, consumers worry that their information could he misused by both authorized and unauthorized users. Within the general debate regarding privacy and confidentiality of health records. this chapter analyzes the demands of health consumers to control the use of their own health data within health management information systems.

THE DILEMMA

The development and implementation of managed health care plans depend on information about individuals in order to determine who should be enrolled. to set rates. to determine quality and effectiveness of services, and to engage in prior and concurrent review. Personal health data have become a refined commodity that has considerable worth in the health care marketplace. Most important. the capacity to transmit patient-specific information within the network of provider; greatly benefits consumers. Access to computerized in. formation con integrate individual care rather than ksep each medical episode a discrete. unrelated event (Petrila, 1996). For example.

the name of a person's psychiatrist or medication records could be available instantly to doctors in a psychiatric emergency room. even though the individual who is being evaluated might not be able to provide this *information.* Also. the repeated collection of a person's medical history could be eliminated. saving the staff and the consumer much time and effort.

However. people care deeply about their medical information. It is personal. The risks of exposure of medical records that can profoundly change people's lives are multiplying. With increasing frequency, the public reads or hears of cases in which individuals have lost insurance. jobs. and housing or have been subjected to public humiliation because of something in their medical records. "Whether HIV. cancer. diabetes. or some other health problem. companies are using the information to decide who gets hired. fired. and promoted" [Stanley & Palosky. 1997d). The following incidents are just a few examples taken from an in-depth series of articles on medical privacy published in *The Tampa Tribune* (Palosky & Stanley. 1997a, 1997c; Stanley & Palosky. 1997d):

- A Tampa woman never expected anyone to learn about her sessions with a therapist, but when she got hurt in a car accident and sued. defense lawyers claimed that her problems were mental. not physical. At the trial. an attorney read to the jury from the therapist's notes the details of her past emotional problems. "I looked like a crazy person. and I lost the case." reported the woman.
- In California. a state agency denied a man a job in part because he had been treated for depression.
- When Rep. Nydia Velaquez (D-NY) first ran fcr Congress in 1992, the New York *Post* published details about her past suicide attempt. She won the election and later sued her hospital for failing to protect her records.
- The names of 4.000 people on a Florida state-created list of AIDS patients were copied from a state computer and mailed to newspapers.

Inadvertent breaches of confidentiality. health data searches by law enforcement agencies. and the myriad of data-merging activities that are taking place have crested a chilling effect on people who seek medical help. Stigmatized populations. such as people with mental illness, HIV/AIDS. or alcohol and substance abuse problems. are the most vulnerable to violations of health privacy because the practical consequences of being identified are extreme.

In general, medical privacy issues of a person who has bipolar disorder do not differ substantially from those of someone who is HIV positive. Not only have such people been victimized by their disease, but they also have been forced to confront attendant prejudice, discrimination, and public fear. Medical privacy, therefore, looms over their everyday lives and must be addressed within the critical context of civil liberties.

ACCESS TO DATA

It was not long ago that transmission of a medical record meant that the file was put into a pneumatic tube and sucked away to another part of the hospital. Clinicians' handwritten progress notes, which once were kept in manila folders in locked file cabinets, are giving way to vast electronic warehouses that store, integrate, and link data. The growth of a national health data infrastructure coupled with technological advances in electronic data management provide health care systems with the capacity both horizontally and vertically to integrate, synthesize, and use health information with few restraints (Gostin, Lazzarini, Neslund, & Osterholm, 19961. Most of this is bring accomplished without the knowledge or permission of health care recipients (Campbell 1997b)

Privacy *and confidentiality* for the individual consumer implies that access to personal health data and clinical records is limited by informed consent, the law, medical ethics, and state and national policies that protect the consumer, the consumer's family, and the provider agencies that collect and manage data and clinical records. However, as the power of information systems grows, ethical, financial, and technological dilemmas emerge to challenge such protections. Most people do not realize who sees their medical data. Harvard law professor Arthur Miller said, "It's like the genie springing out of the bottle, going anywhere on the planet for any purpose whatsoever" (Stanley & Palosky, 1997a). Self-insured employers often review medical information such as doctors' bills and prescription records to track their health plan's expenses. Health maintenance organizations often require detailed data about patients before they approve treatment. In some states, regulators collect social security numbers (SSNs) and other data about every person who enters a hospital or an alcohol/drug treatment center.

Furthermore, with the emphasis on patient tracking and controlling health costs through outcome-based decision making, the potential for misuse of health data in services research has increased enormously. Researchers have liberal access to records, in-

cluding those of people with stigmatizing conditions. The trend to. ward increasingly rigorous evaluation of services through research in the community and in institutions and the expanding influence of consumers, family members, and advocates in the research end data collection arena have clouded traditional protections and compromised boundaries of taken-for-granted ethical authority and Protocol (Campbell & Estroff, 1995). Most attention in the field has been focused on ethical dilemmas in neurobiological research—especially experimental psychotropic drug research (Burd, 1995; Weisburd, 1994)—leaving protocols that protect data subjects in a regulatory gray zone. The important ethical questions that behavioral health providers and services researchers now face in their investigations have seldom been addressed. and the data community has yet to achieve consensus about standards and policy recommendations (Campbell. 1996b).

As the federal government initiates national medical privacy standards that can accommodate the new technologies. it is important to recognize that promises of better services are not persuasive either for the general public or for vulnerable populations. In fact, the causation among linkage of records, outcomes studies. and quality of services has yet to be proved in the scientific community

Public attitudes reflect overwhelming support for more controls regarding medical privacy. The 1993 Equifax Harris Consumer Privacy Survey (Electronic Privacy Information Center [EPIC], 1999) found that 75% of people in the United States worry that medical information from a computerized national health information system will be used for many nonhealth reasons. and 38% arc very concerned. Although most said that it was important that individuals have the legal right to obtain a copy of their own medical record, 85% believed that protecting the confidentiality of medical records is "absolutely essential" or "very important" in health care reform; 56% favored new comprehensive legislation to protect the privacy of medical records. and 64% did not want medical researchers to use their records for studies—even if the individual is never identified-unless researchers first get the individual's consent. Of those surveyed. 96% supported federal legislation that would designate all personal medical information as "sensitive" and impose penaltics for unauthorized disclosure. The "Live and Let Live" American Civil Liberties Union (ACLU) pull in 1994 also found that 75% of those surveyed are concerned a "great deal" or a "fair amount" about insurance companies' putting medical information about them into a computer information bank to which others have access (EPIC. 1999). Similarly, a 1996 CNN poll found

that 87% of Americans believed that patients should be asked permission every time any information about them is used (EPIC, 1999).

It is clear that an improperly thought out and implemented data system can result in invasion of privacy, personal surveillance, abridgment of constitutional rights, inappropriate monitoring and control of individuals, and access to personal data for private profit or criminal use. Besides anxiety about information leaks, most people have a natural reluctance to be tracked and monitored in the most personal aspects of their lives. By expanding the scope and capacity of electronic information systems, personal autonomy is eroded even when records can be secured. Both of these types of privacy concerns produce adverse medical and public health consequences. People do no, tell the whole story to doctors when they fear that they or their friends and relatives will be harmed as a result of leaks in the health information system or that "Dig Brother" is watching. It is the expectation of privacy that leads to trust in the doctor–patient relationship Without the confidence that a physician will hold private the most intimate facts of a person's life, patients do not reveal themselves. Consequently, treatment can 'be hindered or delayed. In testimony to the National Committee an Vital and Health Statistics (NCVHS), George Flores, M.D. 119971, a public health professional, stated.

> Public health holds an unique position in access to and the need to work with sensitive client information. In order to be able to make contact with parsons having contagious conditions and to have the cooperation and trust of their medical providers, the door to public health must be open to all categories of individuals, including those who may be disadvantaged by disclosure of their identity For the door to be open, there must be public confidence in the privacy and security of medical information. Thir holds true for medical as well as mental health clients, their medical records, and, in many cases, their identities.

Mental health consumers share similar concerns regarding medical health privacy with those who have illegally immigrated to the United States. Some people with mental illness choose to stay away from **mental** health services because they also fear that an encounter would put themselves, a family member, or a friend in a threatening position. They could potentially be stigmatized and the information used against them to deny work, custody of children, or even freedom. However, not seeking services could cause an exacerbation in symptoms for people with mental illness, putting themselves and others at risk. The point is that lack of privacy assur-

ances in health data collection has been shown to adversely affect help-seeking behaviors and. subsequently. precipitate public health problems.

Protections and issues of control of access to medical records are not rigorously evaluated in terms of their impact on health consumers, and consumers' voices often are not represented when standards are being developed. Health privacy ultimately is a struggle over control of health records and is more *related* to *issues* of informed consent and ownership of records than to security. What is ironic is that security concerns and recommended protocols for electronic health records restrict consumers' access to their own records but do little to control the use of the records in management information systems. In fact, most efforts to develop medical privacy standards in the United States proceed from the assumption that access by third parties, including Provider networks, billing companies. law enforcement, and researchers. *is* necessary, and most protections being drafted accommodate demands for data linkage end transmission.

Beyond issues of security and controlled access to medical records. other struggles are being waged under the banner of medical privacy. Obviously. ideas and perspectives are powerful tools of both social change and control. especially when they are coupled with data. The production al medical information has had considerable influence on determining health policies related to treatment and cost. The corporate and public behavioral health systems that manage medical records may have vested interests in restricting information that reflects negatively on their organizations. Such data have the potential to validate criticism of health service delivery systems, Where data often serve to justify the status quo, issues of data access and control provide fertile ground for a discussion of values and the attitudes and behaviors of professionals in executing data collection protocols end distributing results of performance-based studies (Campbell & Estroff, 1995: Petrila, 1996: Wedding. Topolski, & McGaha, 1995).

If the *sense* of what *is* right is equivocal and *dialogue* is submerged in taken-for-granted practices. then who or what policy mechanisms are capable of defining ethical codes or developing surveillance systems to monitor *discrete* behaviors within the data collection process? With privatization of health care has come the weakening of the oversight and regulatory roles of the federal government. Furthermore, data conflicts involve complex reciprocal social and personal relationships. How are choices negotiated between individual gain end the greater good. or individual good and

the greater gain? Do the ends now justify the means as efforts to manage by outcomes suggest? Following orders of superiors and sometimes even engaging in unethical behaviors are rewarded in health care entrepreneurialism, whereas whistle blowing or making an individual choice to break an unjust law spells corporate death.

History teaches that principles of "The Good" or "The Right" are not necessarily consensual but rather political. They flow from the top down through the state and bureaucratic structures, where they are codified in law, contract language, or become part of a set of informal protocols. However, what may be most compelling in prescribing standards of behavior and practice is the weight of aggregated private decision making of middle-level managers on public and corporate policies. Private fears and desires for gain or recognition become a latent infrastructure, invisible to the system at the organizational level but manifest to individual participants as "the rules of the game." Protecting medical privacy becomes a colluded process that is situational and self-justifying. Protections and protocols. while grounded in custom and organizational history. are actually reflective of personal acts Expressed as organizational will [Campbell. 1997a)

Mandating privacy protocols and technologies packed with security features is useless if people do not aggressively use these strategies. Although rules and regulations can provide pressure to control abuse, compliance inextricably will be subverted without the development of a profound respect by all constituencies for the value and worth of individual consumers. One need only to look at the violations of privacy end confidentiality that occur daily from the cavalier way that people handle and transmit data within low-tech systems to understand the nature and magnitude of the problem within electronic data infrastructures. Tha nature of privacy compliance problems arc illustrated in the following account:

> While working at a state department of mental health, I encountered considerable resistance when I attempted to institute privacy protections around the use of a facsimile machine that received consumer-specific information, As I walked through the central offices, I often found lists of the names of patients at the state hospital lying in the fax machine or roiled up on the floor. I was the only one who seemed to notice or to care. When I recommended that a fax machine dedicated to receiving such information be put in a locked room or that client-specific information not be transmitted by fax, the only accommodation made was to place a portable room divider around one side of the machine.
>
> Later, at a research institution where I was subsequently employed. I observed that surveys of mental health consumers with respondent names on the cover sheets were routinely left in plain sight in an un-

> locked room. Again, I was the only one who seemed to notice or to care. I reminded people that informed consent of consumers to participate in the survey was a contract between the respondents and the researchers who promised that the surveys would be kept in a locked file. Eventually the door was locked, but when electrical repairs to the room were made, a desk from that room with a red file labeled "Confidential Client Information" sat on the desktop in the hallway until I finally *removed* rhe file and rook it to my supervisor. (J. Campbell, personal observation, 1997)

From such experiences, one can begin to recognize that many people do not connect mental health data with individuals. By carelessly handling someone> mental health record, people fail to realize that they are treating that person in a disrespectful, dehumanizing manner. Protection of privacy and confidentiality of mental health data becomes a collection of rules and protocols that people begrudgingly follow; they are not necessarily vigilant. Perhaps it is the stigmatized role of consumers and the "them and us" mentality of professionals that sustain a general lack of genuine concern within the culture of mental health services research.

The inherent tension around who should have access to health data and issues of confidentiality of health records have vast implications for the production and distribution of health information. but data collection policies and protocols also have an impact on *the* development of the cultural reference points that underlie every aspect of the personal and social relationships between profession. als and consumers in the data collection, storage, and utilization process. Ultimately, the social relationships of health data management have the potential to alter the symbolic processes by which a consumer's reality is produced, maintained repaired, and transformed. For this reason alone, the rights of consumers should be put first.

CONSUMERISM VERSUS PATERNALISM

The growing tide of health consumerism is one of the most compelling forces in carving out a role for mental health consumers in the production, storage, and use of their health data. It is based on the assumption that people who seek health services are customers just as are people who seek other types of services. The doctor is perceived to be the purveyor of a service, and the patient is viewed as the buyer. The consumer listens to the thoughts of the provider but ultimately makes his or her own decisions. *Consumerism* implies that values derived from principles of good medical care must be interpreted and operationalized through reference to the pa-

tient's personal health care values and desires (Beisecker & Beisecker, 1993).

Although consumerism has periodically emerged as a force in American society, its application in health care draws its roots from two marketplace trends: consumer rights protections, with its concerns regarding manufacturing and product safety, and total quality management, with its focus on customer satisfaction. The former is grounded in individuals' profound distrust of the actions and motives of providers of products and services; the latter promotes collaboration between provider and consumer and seeks to answer such questions as, "What do customers prefer?" It is important to recognize that both trends emphasize the need for information that accommodates consumer rights and interests.

Contrast this vision of consumerism with the fear, anger, and sadness often conveyed when people speak about violations to the privacy and confidentiality of their own health records. These experiences stand as a robust critique of management information systems and consumer rights and protections in health services research. It is not surprising that managers and scientists have been unable to cope with growing demands for changes in the data management process, particularly those that come from people with stigmatizing conditions and from their families. Paternalism, not consumerism, would appear to remain the reigning ethos in the management of health information. The American Psychiatric Association has repeatedly lobbied Congress when health data access and confidentiality legislation was being considered to prevent a person's access to his or her personal psychiatric records. Such restrictions on access have been legislated by many states and are supported in *Confidentiality of Individually-Identifiable Health Information: Recommendations of the Secretary of Health and Human Services, pursuant to section 264 of the Health Insurance Portability and Accountability Act of 1996* (U.S. Department of Health and Human Services [DHHS], 1997). Mental health professionals fear that giving broad access rights to mental health consumers may pose a danger to an individual's psychological health. As with science in general, psychiatric research is bound by the past and inscribed with power, bias, and stereotypy. Reform in research methods, protocols, and human subjects' protections historically has been based on the assumption that "the expert knows best" about the operating principles of research. Furthermore, scientists believe that they know the values *and* preferences of their subjects, that they are disinterested and objective without biases of their own, and that they can choose for their subjects what the sub-

jects would choose for themselves if they had the same knowledge. This seduction by authority inevitably influences future behavior to mimic current practices and thus leads to the creation of data protocols and protections without knowledge of how consumers would address these issues.

REIFICATION OF SYSTEM VALUES

One of the most disturbing claims to override consumers' rights to confidentiality is the need for outcome studies. Such studies not only may involve the use ofpsychiatric records without consent but also may require that service recipients fill out intrusive question. naires as a condition of their treatment. Consumers question the value of this type of research and ask whether system values-in this instance, the potential for lower costs and more effective treatment modalities--trump the value of respect for individual autonomy. In response to Nazi atrocities in the conduct of human experimentation. the Nuremberg Code proclaimed as its first principle that "the voluntary consent of the human subject is absolutely essential" [Katz. 1972, p. 305). One of the most well-respected historical documents concerning the use of human subjects in medical research, it requires that "the person should be able to exercise free choice without intervention of any element of force or coercion" (p. 305). Scientists who justify the widespread use of outcome studies are really amending this fundamental premise of patient consent for research by advancing public goals. If outcome studies and other services' research activities were included under human subjects' protections. then individual benefit—not public benefit-would have to be weighed by the consumer against potential risks of data collection in an informed consent protocol.

Fearing loss of enrollees, contracts, and public scrutiny. administrators of public and private health delivery systems are claiming proprietary rights of data ownership to control access to information (Petersen. 1995). Often, when public agencies and private companies pay for data collection, they demand the right to prohibit the review or publication of health service system information without their permission. Slate mental health authorities may impose similar limitations on researchers as to the presentation. publication. or review of data, and access to services research is denied to the public when results are potentially unfavorable. In there ways, academic freedom end the public's right to know—even when federal and state money is used-are silently being undermined by system-centered concerns regarding disclosure of information.

Finally, there is an eagerness by those in politics to reveal personal health information to gain advantage, and instances in which privacy protections have been put aside in the service of public policy are not new. This complicates the role of government as the protector of medical privacy. Consider the case of Daniel Ellsberg (Hayden, 1988; Robitscher, 1981; *World* Book *Year Book*, 1974; Zinn, 1990) The first public act in the Watergate cover-up was not the break-in at the Watergate Hotel, but a break-in 9 months earlier for psychiatric information to discredit Ellsberg, who had turned against the Vietnam War. Ellsberg had copied volumes of secret Defense Department papers and made them available to *The New* York *Times* while he was working for the Rand Corporation, as a government consultant He said that he released the information because the American people had a right to know about the actions of their government. The Supreme Court upheld the right of newspapers to print the material, ruling that the government's attempt to suppress publication was "prior restraint of freedom of the press" and, therefore, unconstitutional. However, Ellsberg was still indicted for espionage, theft, and conspiracy. Ultimately, the case was dismissed after 89 days because of a number of violations of procedure, including the illegal break-in at the office of Ellsberg's psychiatrist. The judge labeled such behavior as "improper government conduct, shielded so long from public view" that offended "a sense of justice" (*World Book Year Book, 1974,* p. 307).

Proposed legislation might well allow federal and state agencies the vary type of access that once was gained only through covert activities. It has been reported that recommendations by the Clinton administration regarding medical privacy would permit health care providers and those who pay for such services to be explicitly permitted to disclose health information without authorization when the records are sought by federal or state Investigators. Furthermore, as part of the Brady Handgun Violence Prevention Act (1993), a national computerized background check will include access to psychiatric hospital records to prevent people who have been hospitalized from purchasing handguns (Applebaum & Monahan, 1994).

Because vested interests, bureaucracies, and corporate entities have greater opportunities to affect health privacy policies than do individuals or public advocacy groups (Breitenstein & Nagel, 1997: Nagel, 1998), government agencies are inhibited from rigorously promoting standards and penalties that give priority to individuals to determine appropriate access and use of medical information. The institutions that control information define by default or feel

empowered to determine appropriate use and to minimize the concerns of private citizens. Consequently, administrators strive for as much access to information as possible, and data warehousing and merging technologies rapidly develop to meet the demand. There is little vision or incentive to develop systems that facilitate broad end meaningful consumer control of health records. Rather, services research designs and electronic health information architecture are considered unable to accommodate consumer demands. The creation of a national review body to provide oversight of medical records privacy and respond to health consumer concerns was rejected by the National Committee on Vital *and* Health Statistics in its recommendations to the Secretary of the DHHS because "no clear and practical solutions" (NCVHS, 1997. p. 26) are offered as rationale, with little interrogation of the underlying assumptions for this *position* or alternatives sought.

PUTTING THE RIGHTS OF CONSUMERS FIRST

It is evident that health consumers prioritize their needs for control over their personal health records above any needs promulgated by the government, researchers, or private industry. However, when the dialogue is shined away from individual consumers to discussions of people at the system level, calls for a delicate balancing act between giving organizations what they need to know and individual tights repeatedly surface (Gates, 1998; U.S. DHHS, 1997). The argument is that widespread abuse can be controlled and health privacy can be regulated. When used and secured properly, electronic medical records can help patients and serve the public benefit. Therefore, privacy rights should never be absolute, and policy makers should chart a middle ground between those who wan, unfettered access and those who want stricter safeguards to ensure individual control over any use of one's medical record. The problem is that the concerns and solutions of health consumers as reflected in the national polls, and surveys have not adequately weighed in on the debate. Any abstract balance that is championed is strictly in the eyes of those at the table.

Rather than a shared reality based on market relations, data collection represents two quite separate worlds, and the meanings of one are significantly different from the other. Separated by role and function from the consumer, both public agencies and private corporations construct a rationale that tends to be antagonistic to individual rights to medical privacy.

What emerges when balancing the rights of health consumers with the demand for more personal medical data to be stored and moved electronically is a turf war over controlling human beings in a landscape that includes an entire array of options and widely divergent goals and definitions of fair Information practices. The same policies appear as positive from one perspective. negative from another Whnn defining the cost and feasibility of protections and rights. most stakeholders look at the way it affects the system, whereas the individual consumer will ask. "What does it da to my life?"

For example. researchers will often protest when issues regarding privacy and confidentiality create barriers to their research but may reverse their opinions when health privacy protections affect them directly as a health consumer. Consider the following anecdote.

> A:, a member of a group reviewing grant applications, I found that my persistent concerns regarding the human subjects' protections were met with irritation. However, when we discussed a proposal for a data warehouse that would have direct impact on the medical records of some of the reviewers themselves, the mood changed dramatically. (J. Campbell. personal observation, April 1996)

In this case. the capacity to track people with behavioral health care problems was considered more important to the researcher than the individual rights of "those people" until the issue was made personal.

Because people judge benefit and harm of medical information systems by the impact on the quality of their individual lives, it is the individual perspective that needs to be RI the core of the debate on medical privacy. However. individual concerns are often marginalized to infrequent opportunities for input at public hearings or shuffled aside in misdirected letters or telephone calls that go nowhere.

WHOSE DATA ARE THEY ANYWAY!

To empower individual health consumers to reposition their concerns within the center of power. it is necessary to introduce to the policy-making process the concept of consumer ownership of medical records (Campbell. 1996b). Rather than beingregarded as health partners. consumers feel that that their mental health experiences are really viewed as raw data that can be mined. processed. and sold by entrepreneurs, corporations. and academia without much care for the welfare of the individual (Campbell. 1996b). In fact. it is

rare that consumers are reimbursed for the burden of answering hours of questions for quality management or outcomes research, and they do not share in the profits--whether financial or professional. The situation is akin to a form of colonialism. Consumers are treated more like a captive population whose insights and practices are considered the property of the developer than a market exchange relationship of customer and service provider.

In the novel *The Deus Machine*, Ovellette (1993) created a near-future scenario of the first serious attempts to integrate the government's computer networks and the reaction from groups concerned with protecting the individual's rights to privacy. That fictional struggle was resolved through legislation that declared that personal data were extensions of "person" as defined in the Fourth Amendment to the Bill of Rights. Therefore. health data were protected against search and seizure. and officials were required to obtsin a search warrant before linking end integrating data. The author asked the reader to think of health care data as en individual's personal effects. es something unique with private meaning and value. rather than as a saleable commodity belonging to a corporate or governmental agency. In the struggle over control of individual medical records, mental health consumers are beginning to advance proprietary arguments (Campbell. 1996b). Although there is es yet little case law to support such claims to data ownership. consumers are engaging the legal system as a means to protect and control the use of private health data, to gain access to and direct the collection of system-level information. and to share in the profits from data production end use. Most important, they seek a forum to become leaders in the development of health information system protocols and protections to accomplish these objectives.

PAVING THE WAY OR PROTECTING THE INDIVIDUAL?

When the Health Insurance Portability and Accountability Act (HIPAA) of 1996 (Pl. 104-191) created portability and more coverage for preexisting conditions. it added et the last moment a provision to facilitate the computerization of medical records in national databases run by the government and private corporations. Congress. with the advice of the NCVHS, directed the Secretary of the DHHS to make "detailed recommendations on standards with respect to the privacy of individually identifiable health information" in HIPAA, section 264(a). In making those recommendations, the Secretary is required in section 264(b) to address at least the following: "(1) the rights that an individual who is the subject of individually identifi-

able information should have: (2) the procedures that should be established for the exercise of such rights: (3) the uses and disclosures of such information that should be authorized or required."

Since 1997, the NCVHS has focused almost exclusively on policies for the use and disclosure of individually identifiable health information with requirements to notify the health consumer. replacing rights of informed consent in many instances (U.S. DHHS. 1997). As pert of this agenda. it intends to impose a unique health identifier for everyone so that private medical records can be easily accessed. A report titled "Records. Computers. and the Rights of Citizens" advised the Department of Health. Education and Welfare more than 25 years ego that, "in practice. the dangers inherent in establishing a standard universal identifier--without legal and social safeguards against the abuse of automated personal data systems—Far outweigh any of its practical benefits" (U.S. Department of Health, Education. and Welfare. 1971) In response to the passage of HIPAA. Don Haines. the Legislative Counsel of the ACLU in Washington, D.C., has warned. "This bill will bc remembered by Americans no, as health care reform but as the thief who stole from us the privacy we deserve for our most confidential medical information" (Rosofsky, 1996. p. 2).

PERSON-DRIVEN PROTECTIONS OF HEALTH DATA

Americans do nor want new rules permitting use end disclosure of identified health information, They want to be genuinely protected and their individual medical privacy *enhanced* through "the enforcement of long established privacy principles based on constitutional and statutory law. common law. the Hippocratic oath. the canons of medical ethics. and common sense" *(Health privacy issues.* 1997; Nagel, 1998, p. 1). In the computer age. the risks of data collection cannot be separated from the medical interventions that it documents Therefore. polices and procedures for the protection of human subjects within a health data system. including the rights of privacy and confidentiality in research. evaluation. outcomes management, and quality assurance, should be mandated. In data integration activities. human subjects' protections accorded to research subjects should also apply. Following are some of the most important recommendations advanced by consumers and advocates to protect medical privacy. These privacy recommendations have emerged though consumer focus groups (Consumer/Survivor Mental Health Research and Policy Work Croup. 1992; Trochim. Dumont. & Campbell. 1993). consumer-generated State Mental Health

Agency information policy document> (Kentucky Center for Mental Health Studies. Inc.1998: Maine Department of Mental Health and Mental Retardation. 1993). and policy research (Campbell, 1998). Although these recommendations are particularly critical for protecting stigmatized populations, national polls indicate overwhelming support *of all* Americans for the protections discussed here (EPIC, 1999).

Informed Consent

Al the core of privacy protection that health consumers want is the concept of informed consent. Consumers want to control the use of their records and want the sharing of health information to be voluntary. Therefore. any use of medical records in a person-driven system would require the consent of the consumer. The inclusion of consumer data within electronic databases of unified records or management information systems would also be voluntary end follow informed consent protocols. Some advocates have suggested that psychiatric records not be included in any system of electronic records (Rotenberg, 1994). Without specific informed consent. clinical records should not be retrospectively integrated into an information system. Data sharing and integration between agencies and systems may pose problems with regard to breaching both consumer and family confidentiality. An informed consent protocol regarding release of information between agencies or for storage in a data bank should br required before any data are synthesized or integrated.

Consent is contingent on the consumer's receiving information about the risks and benefits of the use and making an informed decision Such protocols allow consumers to weigh not only the risks but also the benefits (e.g.. better services, information to consumers, access to one's own records, payment for data) for providing information and to waive voluntarily certain protections or security measures for those benefits.

For consent to be truly informed, three factors must be considered: the quality of the information provided, the competence of the consumer to give consent, and the level of coercion to induce consent. Because informed consent protocols are usually written by researchers or administrators, conflicts of interest exist between the nerds of the system and the needs of the individual consumer. To the researcher or administrator. the consent is sometimes viewed es an obstacle to convincing the consumer to agree to the data collection or use. Information in consent forms may be biased or inadequate. Furthermore. the request for consent to use medical records often comes from a busy clerk upon the consumer's admission to a service

provider. Informed consent forms are buried in other paperwork. and people are routinely asked to "sign here" without explanation.

Surrogate consent may be appropriate depending on the competence and conservatorship status of the consumer. However, competence is not a precise legal term. In some states. the courts have ruled that involuntary patients in a psychiatric hospital are considered competent to refuse treatment.

Without consent. services can be denied under current laws With consent. a person's records may be sent to a wide range of users who may not have adequate security. When health plans started demanding private information about patients. the Massachusetts Medical Society proposed perhaps the broadest privacy protections in the country. It said that patients should not be forced to give insurers blanket access to medical information in exchange for health coverage. "We don't believe in coerced consent. Right now that's what patients give" (Stanley & Palosky, 1997b), announced the society's president. Any informed consent protocol that is designed to protect the consumer would have to remedy these problems to be effective.

The Option Out of the System

If services should not be denied to consumers who decline to give consent, then consumers need to be able to "opt out" of an electronic record system (i.e., the organization would keep a person's health records in paper form with some limited exceptions). Researchers have argued that incomplete data and bias could be introduced into outcome studies if this option were adopted. However. this claim is not based on any field research to determine how many consumers would opt out. or on whether the number would be constant, be based on respondent bias. or be reflective of organizational policies that would cause consumers to mistrust the information system, If the consumer believes that the benefits for inclusion outweigh the dangers and if the consumer trusts the organization to keep medical records secure. then few may take the option to stay out of the electronic information system. In fact, the number of consumers who opt out may be a good performance indicator of the information system.

Access

Consumers want full access to all personally identifiable medical records. No records should be kept secret from the consumer. Access to clinical and management information system data by service recipients should be supported wirh protocols developed for indi-

viduals to review and emend their records or to remove any inaccurate. irrelevant. or out-of-date information. Paternalistic medical systems consider access to personal health information part of the privilege and obligation of the doctor to protect the patient end often don't give patients access to their own records. Rather than build trust, this orientation weakens the bond between doctor and patient. Consumers fear what may be in their records. and misinformation ha, caused considerable harm in some cases.

Understandably, there is resistance in health organizations to allow service recipients to review their medical records. Information in the medical records could be misunderstood by the patient and in some cases, create greater liability risks for the health provider. Some mental health clinicians believe that a patient's progress could be harmed if he or she could read treatment notes. Such strategies as failure to notify a consumer of the right of review. excessive charges to the patient for copies, and lengthy waiting periods for records abound. The nature of electronic information systems has created opportunities to erect even greeter barriers. Conversely, electronic information systems could just as easily be used to create opportunities for greater access end ease of access. With proper security, consumer access to personal medical records could help io improve the quality of the information in those records. Furthermore, consumer information used for polity and decision support. particularly de. identified. aggregated figures related to service information (costs, utilization, effectiveness, and consumer satisfaction with services), could be made public and accessible to all citizens. Therefore. electronic information systems could build in accountability to consumers at both the person level and the system level.

However, third-party access to medical records should be strictly limited to a need-to-know basis. Billing agencies should receive only encrypted information. and this information should be destroyed in a specified time period. Law enforcement officials should be required to obtain a warrant after showing a compelling government interest for each piece of information sought. Although privileged communications should never be disclosed. use of even the most general information to sell products to consumers without their written consent should also be banned. A drug store. for instance, would be prevented from contacting people who are taking psychiatric medications to pitch a new treatment or from selling their database to a pharmaceutical company.

Security

The methods used for data storage and distribution should be explicit, and storage and distribution practices should be audited pe-

riodically for compliance Records in storage or transit should be encrypted. Audit trails should track each access to an individual's file. Policies and procedures should also be developed for the protection of consumer confidentiality when using cellular phones. facsimile machines. automated information systems with multiple access points. and other technologies that are used to store, analyze. and transmit information Faxing has become an increasingly common means of sharing information. and although there are no hard numbers. it appears common for confidential medical records to be faxed to the wrong places. For example. one person. whose telephone number is one digit different from a diagnostic center's, received in a 2-year period faxes of medical records for 50–60 people. including 15-page medical histories. These faxes included patients' names. SSNs, and health insurance information. In some cases, there also were addresses and telephone numbers. When this person finally contacted the center and told them that they had the wrong number. she thought that she had solved the problem. Every hospital. tab. and doctor's office that regularly faxed to the center was contacted, but the faxes kept coming [Stanley & Palosky, 1997c). A consumer who is concerned about a health provider's faxing his or her medical records should be able to prohibit the provider from faxing. Also essential to security of records is proper training of personnel. All staff within an organization should be trained in the proper handling of confidential data and regularly evaluated on their performance.

Following the concept of "as much information as necessary. as little information as possible," another approach to protecting health information is to reduce the amount of information by collecting only what is essential. It is possible to reduce absolute risks to data security by collecting outcomes data on random samples rather than on entire recipient populations and by minimizing the amount of data actually collected per respondent, Furthermore. technologies such as virtual systems that use object technology may be able lo replace data warehouses. These virtual systems would allow records to remain at their primary site and be linked only on request. Therefore. it is possible for the consumer, via an authorization protocol. to control the information that is available to the doctor (Work Group for Computerization of Behavioral Health and Human Services Records, 1997).

Privacy and security assurances under law should apply to all users of the information, When health information is transmitted to a third party, the recipient should be required to honor the same privacy and security assurances as the record's original holder, The *Final Report of the Legislative Survey of State Confidentiality Laws,*

with Specific Emphasis on HIV and Immunizations suggested that the duty to protect data be "transferred simultaneously with the data, as would liability for violation of privacy or security standards" (Gostin, Lazzarini, & Flaherty, 1996).

Unique Identifier

Many systems call for the use of the SSN as a consumer identifier and assume that it is both possible and legitimate to convince consumers that the use would pose no risk or minimal risk to tht privacy of an individual. However, consumer privacy under such systems cannot be totally safeguarded (*Protecting* the *privacy 1992;* Ziglan, 1995). The widespread use of the SSN has seriously eroded personal privacy. The growing amounts of information that different organizations collect about a person can be linked because all of them use the same key to identify an individual. Chaum wrote, "This idsntilisr-based approach perforce trades olf security against individual liberties. The more information that organizations have, the lass privacy and control people retain" (1992, p. 971. Personal security is also endangered through the use of the SSN as backers and thieves routinely mine organizational databases looking for people to victimize. Given the stigma associated with mental illness and other disorders, using the SSN or any universal identifier not only poses substantial risks but also constitutes a barrier to access for those who ate unwilling to take the risk Using a person's SSN as a unique identifier should, therefore, be discouraged.

There are alternatives to using the SSN. One of the most promising is the "digital signature" on a smart credit-card-size computer containing memory and a microprocessor. The owner can control the data that are stored and exchanged by incorporating a keypad and display on the card. It would also be possible to incorporate fingerprint identification technology within the card itself to prevent anyone other than the owner from using it. The growing availability of such technologies argue against the use of a unique identification system and especially the use of the SSN. In a person-driven information system, concerns about identifiers would be acknowledged and validated. If unique identifiers arc used, then only minimal information should be anchored to the identifier.

Data Removal

Once a person's health information is in a system *file*, it is usually there for life. This is true whether it is a paper file or an electronic file. However, electronic systems pose a greater danger because information is more easily accessible, regardless of age of the records

and is accessible to a wide range of electronic network users. That means that if a person was in a psychiatric hospital, then a record of that admission would follow the consumer throughout his or her lifetime. It becomes a significant referential point for all clinical decisions in the future. In Maine, the court ordered the Department of Mental Health to notify all patients of the state psychiatric hospital during a certain time Period of a legal decision regarding the department. Even though many people did not want to be found. records ware pulled and merged with the motor vehicle license database. Letters went out bearing the Department ot Mental Health return address on the envelope. As a result some people were "outed" to their family and neighbors For others, it was a difficult reminder of an episode that they wished to forget (J. Campbell, personal observation, August 1996). Mental health consumers want time limits on data storage to Lie specified and data destruction and removal protections to be developed and implemented when a person no longer receives mental health services Procedures should also be developed and implemented for consumers to disenroll from an information system (except for minimal necessary data required to deliver services) without panalty This is especially important when the information system has proved to have inadequate security or the organization has misused medical records.

Review Boards

Reviewing regulations imposed by review boards on health research reveals an implicit assumption that evaluation and outcomes data collection pose minimal risk to participants (Barrows & Clayton. 1996), but subjects report that there has been considerable abuse and that greater risks are involved than most researchers realize (Campbell & Frey. 1993. *Protecting the privacy*, 1992).

Policies and procedures similar to those for research subjects should be developed for the protection of human subjects within the data systems. and a review panel should evaluate prior to the use of consumer records the adequacy of such human subjects' protections in the collection. analysis. storage, and distribution of information. Data *subjects' protections review* panels should be based in the community. With Institutional Review Boards (IRBs), there is always the possibility for conflicts of interests as institutional culture and a shared ideology that is common to its membership tends 10 support the status quo. With local oversight shared by community members, especially by members of stigmatized or underrepresented populations. the interests of a review panel would be broadened and become responsive to the health privacy needs of

individual consumers rather than health organizations and research institutions (Campbell. 1997c).

Laws and Penalties

Where laws guarantee to individuals medical privacy. exceptions proliferate and penalties are few. Donna E. Shalala, Secretary of the DHHS, announced. "Our private health information is being shared. collected, analyzed. and stored with fewer federal safeguards than our video store records. The way we protect the privacy of medical records right now is erratic at best. dangerous at worst" (Pear, 1997. p. A22)

There is much discussion about the constitutional right of privacy. but in practice, the Constitution has provided little support for medical record privacy claims in the United States. The Americans with Disabilities Act (ADA) of 1990 (PL 101-336) requires that med. ical information be kept confidential and separate from personnel files. but privacy harms are usually redressed *through* private actions, such as contract and tort. and somelimes by state agencies (Institute of Medicine, 1994). Every state and territory provides statutory protection for some types of personal health data maintained by a government agency. Forty-one states report statutory penalties for impermissible disclosures. Of these, 31 report criminal penalties. 18 report civil penalties. and 8 report both. Twenty-eight states provide statutory penalties far unauthorized disclosure of privately held health care information. twelve impose criminal penalties. nineteen create civil penalties, and three allow for both civil and criminal penalties (Gostin et al., 1996). Arrests and prosecutions are rare. however. For example. when a nurse showed to television reporters confidential mental health records from Charter Hospital Orlando South. state regulators suspended the nurse's license. and the hospital sued to stop the nurse and television reporters from calling patients who were named in the records. However. the nurse has not faced any criminal charges (Palosky & Stanley. 1997b). For penalties to be a deterrent against unauthorized disclosure. substantial criminal and civil fines should be imposed for actual or attempted unauthorized access. disclosure. or use of medical information. Individuals should be able to enforce rights and obtain damages and related costs in civil court. Furthermore, an independent agency should be created to conduct oversight and to enforce the provisions of any federal medical privacy law.

Retooling Human Technologies

In efforts to change medical privacy laws, policies. end practices, the marginalization of consumer concerns demands dialogue in col-

laboration with all of the data stakeholders. This is the first step in establishing an ethical center from which the challenges of the new information technologies may be engaged. In fact. public constituencies of people who have stigmatizing medical conditions should be sought out and supported as the jewels of a data-use reform process. Such an effort would go beyond developing law and policy to protect medical privacy. to resuscitating the body politic of a country deeply polarized by market forces. prejudice. and ethical ambiguity. It is clear that neither research protocols nor communication technologies that facilitate health data activities are simply mechanical. electronic. or intellectual tools and protocols that serve the needs of individuals and groups within society. Because reform in protecting medical privacy is limited by the attitudes and social relationships of those that research. manage. and deliver services. it follows that the source of new knowledge to guide the next generation of protections may he in the incongruities between the perceptual and experiential framework of the "experts" and those who receive services.

By listening respectfully and treating data collection subjects with dignity. organizations have the power to bridge the differences between the system and service recipients and to generate new understandings (Campbell. 1996a). Instead of resisting criticism. they should welcome consumers and their families to the process. saying, "Gee. how can we improve?" Individually, each of us would also need to interrogate *a priori* assumptions about data collection and to bring to the table a reflexive understanding of the values, sensibilities, biases. and stereotypes that inform participation.

CONCLUSION

Those who handle health information must go beyond focusing on minimal compliance to privacy regulations to strive for excellence. This means rigorously applying the protections that already exist and monitoring their effectiveness to meet the concerns of health service recipients. To sustain data reform. environments in which whistle blowing is supported as part of a continuous quality improvement agenda need to be established. Medical privacy could also be fostered through development of a gold standard for management information system protocols. One starting point could be the Joint Commission on Accreditation of Healthcare Organizations. which now reviews management information systems and outcomes dale collection in its standards. scoring. and decisions (Joint Commission on Accreditation of Healthcare Organizations. 1997). However. the accreditation process has limits because it monitors

compliance to policies and procedures rather then the outcomes of such policies. Behavioral health delivery systems that support health data professionals who go beyond regulations to develop superior models should also be identified and that information disseminated. In particular. models that establish ongoing partnerships with health consumers or employ professionals with stigmatizing conditions should be sough! out and supported. Finally, training people regarding medical privacy protections and ethics. especially when using case studies the.! exemplify the humen *dynamics* of such issues. should also be built into human resource development activities (Campbell & Estroff, 19951.

At the heart of the mental health consumer *movement* is the belief that the goals of health care reform cannot be achieved without attending to the way individual decisions are made. In response to public demand for health organizations to be more open and accountable. a new vision for health care that is more humane, effective. and accountable can be achieved through the coordinated use of data by all stakeholders. Information technologies have the potential to humanize health care relationships by providing people with access to the most complete knowledge at the time of decision making. allowing recipients of medical services to *partner* effectively in care (Campbell. 1996a).

Business and government leaders must look at the *context* in which privacy protections operate, no! just examine the regulations themselves (Campbell, 1997b). In the management of health data dehumanization naturally occurs. People forget that the objects of statistical inquiry are human beings. By gaining a humanistic focus. information technologies could be retooled to create an open architecture of health knowledge production and distribution This development would present barriers to traditional data collection and use and. in some cases. would restrict the conduct of services research and data management. What is ironic is that these very actions could also lead to better information systems and encourage people to grow as ethical beings.

There is little hope that a data *reform* effort can really succeed if it is antagonistic to the cultural or social practices of those who exercise power within a system. There were human subjects' protections in place in Germany prior to World War II. and scientists justified the brutalization of people without much compunction, seeing them as less than human and expendable for scientific progress. *However.* anyone can prevent a rolled-up fax with the names of people committed to a psychiatric hospital from lying discarded on the floor of an administrative office. The seeds of a

person centered information system would grow from the heroics of everyday life, from people who begin to care enough about themselves as individual health consumers to stop making small compromises by looking the other way.

To prevent an escalation in the fight over access to and security of electronic patient health records and electronic management information systems, a fundamental change in corporate philosophy is needed. The focus on continual quality improvement of individual clinicians and the service system must be encouraged through the collaborative use of information by all stakeholders in the health delivery system. For consumers, fear can be driven out of electronic data collection by developing participatory action research initiatives, establishing data protections review boards with multistakeholder membership, and building trust and incentives for data sharing. As consumers become equal health information partners and data trustees with providers, they will recognize that even the best systems are not absolutely safe from security failures. Health information partnerships will enable the health care industry to move beyond issues of confidentiality and control of health records to embrace the principles of health informatics, or the education of the public by facilitating the distribution of health information. Only by making sure that people's privacy and confidentiality are protected and that people have access to needed health information—both clinical and administrative—can the mental health system effectively engage service recipients in building electronic health information networks.

To protect medical privacy, people must recognize that data reforms-including rules and regulations—are not out there waiting to be found or adjudicated, and society is not driven into the future by technological forces that stand outside social control. The future is contingent on each individual's looking with new eyes at policies regarding medical privacy and climbing for higher ground. In other words, it is the quality of ethical struggles to do the right thing, not particular outcomes, that will ultimately define health privacy protections in the computer age.

REFERENCES

American Civil Liberties Union. (1994) "Live and Let Live" Poll [On-line]. Available: http://www.epic.org/privacy/medical/polls.html

Americans with Disabilities Act (ADA) of 1990, PL 101-336, 42 U.S.C. 12101 *et seq.*

Applebaum, P., & Monahan, J. 11994. July 29). Brady bill's false slap. *The Boston Globe*, 19.

Barrows, R., & Clayton, P. (1996). Privacy, confidentiality, and electronic medical records. *Journal of the American Informatics Association, 3*(2), 139–148.

Beisecker, A., & Beisecker, T. (1993). Using metaphors to characterize doctor–patient relationships: Paternalism versus consumerism. *Health Communication, 5*(1), 45–58.

Breitenstein, A., & Nagel, D. (1997, August 20). Keep your health history private. *The Los Angeles Times*, p. B7.

Burd, S. (1995, January 20). Adequate protection for human subjects? Researchers, advocates for mental patients clash over U.S. rules. *The Chronicle of Higher Education*, p. A29.

Campbell, J. (1996a). Toward collaborative mental health outcomes systems. *New Directions for Mental Health Services, 71*, 69–78.

Campbell, J. (1996b). Who owns the data? *Behavioral Healthcare Tomorrow, 5*(6), 49–51.

Campbell, J. (1997a). Ensuring ethical, accountable systems of care. In D. Evans & C. Harding (Eds.), *Decisions & dilemmas: Local-level managed mental health care* (pp. 21–26). Boulder, CO: Western Interstate Commission for Higher Education.

Campbell, J. (1997b). Privacy and confidentiality. In S. Moffic (Ed.), *The ethical way* (pp. 108–111). San Francisco: Jossey-Bass.

Campbell, J. (1997c). Reforming the IRB process: Towards new guidelines for quality and accountability in protecting human subjects. In A.E. Shamoo (Ed.), *Ethics in neurobiological research with human subjects: The Baltimore conference on ethics* (pp. 299–303). Amsterdam: Gordon and Breach Publishers.

Campbell, J. (1998). *The technical assistance needs of consumer/survivor stakeholder groups within state mental health agencies*. Alexandria, VA: National Technical Assistance Center for State Mental Health Planning.

Campbell, J., & Estroff, S. (1995). *Ethical issues in mental health services research: Technical report series*. Alexandria, VA: National Association of State Mental Health Program Directors Research Institute.

Campbell, J., & Frey, E. (1993). *Humanizing decision support systems: Report to the Mental Health Statistics Improvement Program (MHSIP)*. Rockville, MD: Center for Mental Health Services.

Chaum, D. (1992). Achieving electronic privacy. *Scientific American, 267*(2) 96–101.

Consumer/Survivor Mental Health Research and Policy Work Group. (1992). *Reports 1, 2, 3*. Fort Lauderdale, FL: Center for Mental Health Services Knowledge Exchange Network.

Electronic Privacy Information Center. (1999). *Medical privacy public opinion polls* [On-line]. Available: http://www.epic.org/privacy/medical/polls.html

Equifax "Harris Consumer Privacy Survey" [On-line]. Available: http://www.epic.org/privacy/medical/polls.html

Flores, G. (June 2, 1997). Testimony. National Committee on Vital and Health Statistics. San Francisco, CA.

Gates, J. (1998, Summer). Privacy and confidentiality of health information. *Treatment Today, 10*(2), 7.

Costin, L., Lazzarini, Z., & Flaherty, K. (1996). *Legislative survey of state confidentiality laws, with specific emphasis on HIV and immunization.*

(Final report presented lo the U.S. Centers for Disease Control and Prevention, The Council of State and Territorial Epidemiologists, and the Task Force for Child Survival and Development. Carter Presidential Center (On-line)). Available, http://www.epic.org/privacy/medical/cdc survey.html

Gostin, L., Lazzarini, Z., Neslund, V, & Osterholm, M. (1996). The public health information infrastructure: A national review of law on health information privacy. *Journal* of *rhe* American *Medical Association, 275*(24), 1921–1927.

Hayden, T. (1988). Reunion: *A memoir* New York: Random House.

Health Insurance Portability and Accountability Act of 1946. PL 104-191, 42 U.S.C. 201 §§ *et* req.

Health privacy issues. Hearings before the Subcommittee on Privacy and Confidentiality of the National Committee on Vital and Health Statistics. (1997, February 19) (testimony of Denise Nagel).

Institute of Medicine. (1994). *Health data in the information age: Use, disclosure, and privacy* Washington, DC: National Academy Press.

Katz, I. (1972) *Experimentation with human beings. New* York. Russel Sage Foundation.

Kentucky Center for Mental Health Studies, Inc (1998). *From the KCMHS Notebook: Consumer Guidelines for Research and Data Management.* Lexington: Author

Maine Department of Mental Health and Mental Retardation, (1993). *Draft policy on privacy and confidentiality of mental health data.* Augusta: Office of Research. Quality Assurance and Information Servicer.

Nagel, D. (1998). Outcomes, paving the way to loss of health privacy? *P/C 2000, 3*(2), 1. 3.

National Committee on Vital and Health Statistics. (1997, June 24–25). *Minutes.* Washington. DC U.S. Department of Health and Human Services.

Ovellette, P. (1993). *The deus machine.* New *York: Packet* Star Books

Palosky, C.. & Stanley. D (1997a, February 15). Famous breaches of medical privacy. *The Tampa* Tribune (On-line). Available: http://www.tampa trib.com/reports/medical/home.htm

Palosky, C., & Stanley, D. (1997b, February 19). Computer full of secrets *The Tampa Tribune* (On-line). Available: http://www.tampatrib.com/ reports/medical/home.htm

Palosky, C., & Stanley, D. (1997c, March 21 Readers fear medical secrets a tool *for firing. The Tampa Tribune* (On-line). Available: http://www. tampatrib.com/reports/medical/home hrm

Pear, R. (1997, August 10). Clinton to back a law on patient privacy, The New York Timer. p. A22.

Petersen, C. (1995). PCA takes on Florida's government over disclosure. *Managed Healthcare, 5*(8), 10–13.

Petrila, J. (1996, March). Ethics. The core values of privacy and confidentiality, *P/C 2000, 1*(1), 1–3

Protecting the privacy of social security numbers ond records. Hearings before the Subcommittee on Social Security and Family Policy, Committee on Finance, Senate, 102d Cong., pro forma Sess. (1992). (testimony of Marc Rotenberg).

Robitscher, J. (1981). *The potters of psychiatry.* Boston: Houghton Mifflin.

Rosofsky, J. (1998). The law: Assaults on privacy in Kennedy-Kassebaum. *Practice Management Monthly, 4*(10), 1–2.

Rotenberg, M. (October, 1994). *Keynote address: Seizing the Opportunity: The power of health information.* The American Health Information Management Association national convention, Las Vegas, NV.

Stanley, D., a Palosky, C. (1997a, February 15). Health information industry embraces technology. *The Tampa (Tribune* [On-line]. Available: http://www.tampatrib.com/reports/medical/home.htm

Stanley, D., & Palosky, C. (1997b, February 19). Patients should control data, advocates say. *The Tampa Tribune* [On-line]. Available: http://www.tampatrib.com/reports/medical/home.htm

Stanley, D., & Palosky, C. (1997c, February 28). Fax drops records in her lap. *The Tampa Tribune* [On-line]. Available: http://www.tampatrib.com/reports/medical/home.htm

Stanley, D., & Palosky, C. (1997d, March 2). Employees at risk. *The Tampa Tribune* [On-line]. Available: http://www.tampatrib.com/reports/medical/home.htm

The Joint Commission on Accreditation of Healthcare Organizations. (1997). Comprehensive *accreditation manual for behavioral health care.* Oakbrook Terrace, IL: Author.

Trochim, W., Dumont, J., & Campbell, J. (1993). A *report for the state mental health agency profiling system: Mapping mental health outcomes from the perspective of consumers/survivors. Technical report series.* Alexandria, VA: National Association of State Mental Health Program Directors.

U.S. Department of Health and Human Services (U.S. DHHS). 11997. September). *Confidentiality of individually-identifiable health information, recommendations of the Secretary of Health and* Human Services, *pursuant to section 264 of the Health Insurance Portability and Accountability Act of 1996.* Washington, DC: Author.

Wedding, D., Topolski, J., & McGaha, A. (1995). Maintaining the confidentiality of computerized mental health outcome data. *The Journal of Mental Health Administration, 22*(3), 237–244.

Weisburd, D. (Ed.). (1994). Ethics in neurobiological research with human subjects. *The Journal of the California Alliance for the Mentally Ill, 5*(1).

Work Group for Computerization of Behavioral Health and Human Services Records. (1997, May). *Towards the consumer-focused behavioral health and human services record.* Unpublished report.

World Book Year Book. (1974). Chicago: Field Enterprises Educational Corporation.

Ziglan, A. (1995). *Confidentiality and appropriate uses of data.* Rockville, MD: Center for Mental Health Services.

Zinn, H. (1990). *A people's history* of *the* United *States.* New York Harper Perennial.