Privacy, Consent, and the Electronic Mental Health Record: The Person vs. the System

NORMAN A. CLEMENS, MD

As electronic health record systems become widely adopted and proposals are advanced to integrate mental health with general health systems, there is mounting pressure to include mental health information on the same basis as general health information without any requirement for active, individual patient consent to do so. A prime example is the current effort to change the *Mental Health Information Act of the District of Columbia*, which has, up till now, stood as a model for protection of the privacy of patients with mental illness, the requirement of informed consent for disclosure of health information, and delimitation of minimum necessary disclosure. Mental health information is exceptionally sensitive and potentially damaging if privacy is breached, which makes patients reluctant to seek treatment if they cannot be assured of confidentiality. In addition, there have been spectacular breaches of the security of large electronic health record databases. A subtle but more likely threat is the possibility that mental health information in networks could be fully accessible to all of the patient's providers in a network, not just those for whom it would be necessary to the patient's care. In the 1996 Supreme Court decision in *Jaffee v. Redmond*, the high court recognized that confidentiality is essential for patients to engage in effective psychotherapy, and HIPAA maintains that special status in the protection of psychotherapy notes as well as explicitly stating that it defers to state laws that are more protective of confidentiality than is HIPAA itself. Highly sensitive information also exists in mental health records aside from psychotherapy notes. Any change in the laws that govern informed consent for disclosure of mental health information must take these factors into account. Specifically, the author opposes any change that would assume tacit consent to release mental health information through an electronic health information exchange in the absence of a patient-initiated request to "opt out"; the requirement that the patient give active, informed and non-coerced consent to disclose information—"opt in"—must be preserved. *(Journal of Psychiatric Practice* **2012;18:46–50**)

KEY WORDS: privacy, confidentiality, informed consent, disclosure, *Mental Health Information Act of the District of Columbia*, health information exchanges, electronic health records, psychotherapy, mental health, security breach, *Jaffee v. Redmond*, psychotherapist-patient privilege, Health Insurance Portability and Accountability Act (HIPAA), opt out, opt in

A seismic change in delivery of health care

We and our patients are in the midst of a sweeping metamorphosis of the American health care system. Health care is increasingly concentrated in huge, organized medical systems or managed by a handful of giant insurance companies, with growing pressure for uniformity and compliance with previously developed algorithms in the delivery of services. Associated with this is the drive towards system-wide implementation of electronic health information exchanges, in which all individual patient information is routinely and entirely managed through a central information system. As the interaction of biological and psychosocial aspects of psychiatric disorders becomes better understood, there is a trend toward assuming that mental health treatments no longer carry the stigma traditionally ascribed to them and that they can be "integrated" with general medical care. That integration is presumed to include mixing ("sharing") psychiatric health information with health records from general medical care. Fully integrated records now exist in some major hospital systems and in claims management in health insurance systems such as Medicare, unless mental illness is "carved out" to subcontracting behavioral managed care organizations.

Norman A. Clemens, MD, is Emeritus Clinical Professor of Psychiatry at Case Western Reserve University School of Medicine and Training and Supervising Analyst at the Cleveland Psychoanalytic Center. .

The author acknowledges Barry J. Landau, MD, Paul W. Mosher, MD, and James C. Pyles, LlB, who provided extensive assistance in preparing this article.

DOI: 10.1097/01.pra.0000410987.38723.47

The benefits of these developments are assumed to be self-evident: electronic speed and efficiency, ease of access in critical situations, avoidance of medication errors and harmful drug interactions, access to full medical information when a patient needs care while traveling, availability of aggregated data for analysis and research, eventual cost savings, and so forth. Psychiatric drugs can interact dangerously with other medicines, and psychiatric conditions such as depression and anxiety may profoundly affect diseases of other systems such as diabetes, heart disease, and gastrointestinal disorders (and vice versa). Obviously, there is value in therapists sharing appropriate information from psychiatric treatment with colleagues in general medicine. However, the degree to which these assumptions have actually been tested is not clear. Some, such as the reduction of medical errors, when submitted to study, have not been solidly confirmed. A study by the Institute of Medicine on the safety of electronic health systems in their present state gave the following preliminary conclusion (p. 2):[1]

> For other products—including electronic health records, which are being employed with greater frequency—some studies find improvements in patient safety, while other studies find no effect.
>
> More worrisome, some case reports suggest that poorly designed health IT can create new hazards in the already complex delivery of care. Although the magnitude of the risk associated with health IT is not known, some examples illustrate the concerns. Dosing errors, failure to detect life-threatening illnesses, and delaying treatment due to poor human–computer interactions or loss of data have led to serious injury and death.

There are serious risks in these developments for those who suffer from mental disorders. Some of these risks have to do with the flaws and vulnerabilities of big data systems, and some have to do with the patient's trust in confidentiality within the psychotherapist-patient relationship that is essential to all mental health care, but especially critical to effective psychotherapy. Any threat to the privacy of mental health care poses great risks because patients will either not seek help or will not fully disclose what is troubling them if confidentiality is not assured. In the building of great systems of health care delivery, it is important to bear in mind that the fundamental purpose of these systems is to assure that each individual receives the care he or she needs. Effective psychotherapy, a major treatment of mental disorders that is often provided concurrently with psychopharmacological treatment, depends on each individual's assurance of privacy and confidentiality, and on respect for that person's rights and uniqueness.

Table 1. Definitions from the *Mental Health Information & Primary Care Integration Act

Health information exchange: an electronic system that receives, maintains and facilitates the transfer of protected health and mental health information by and between mental health and healthcare providers.

Healthcare provider: means an individual or entity licensed or otherwise authorized to provide healthcare service, including a hospital, nursing facility, comprehensive outpatient rehabilitation facility, home health agency, hospice program, renal dialysis facility, ambulatory surgical center, pharmacy, physician or health care practitioner's office, long-term care facility, behavior health residential treatment facility, health clinic, clinical laboratory, health center, physician, physician assistant, nurse practitioner, clinical nurse specialist, certified registered nurse anesthetist, certified nurse midwife, psychologist, certified social worker, registered dietitian or nutrition professional, physical or occupational therapist, pharmacist, or other individual health care practitioner.

**The Mental Health Information & Primary Care Integration Act is a bill pending in the District of Columbia.[3]*

A model privacy law under siege

The *Mental Health Information Act of the District of Columbia* has been a model for the country. It requires informed consent for the disclosure of mental health information and sets a standard of minimum necessary disclosure that was the basis for the American Psychiatric Association's publication *Minimum Necessary Guidelines for Third-Party Payers for Psychiatric Treatment*[2]—which in turn has influenced limitations on the type of information that can be disclosed under the Health

Insurance Portability and Accountability Act (HIPAA) with regard to insurance carriers' utilization review. However, amendments to the District of Columbia law have been proposed and are embodied in a pending bill called *The Mental Health Information & Primary Care Integration Act*,[3] definitions from which are shown in Table 1. These proposed amendments would permit "sharing" of information from mental health records without patients' active consent within health systems via electronic health information exchanges (Table 1) In a fact sheet posted on August 8, 2011, the Behavioral Health Association of the District of Columbia described the goal of these changes as follows: "These efforts broadly attempt to allow D.C. agencies and providers to share information without consent, with the goal of improving care coordination and the delivery of governmental benefits."[4] Information would be "authorized for exchange" in the following categories: "Administrative information (date of birth, providers, and insurance information); medications; lab orders and results; diagnoses; CPT codes; presenting problem list; discharge summaries; allergies; radiology reports; immunizations; vital signs and observations."[4]

The proposal to allow sharing of information among those providing care is well intentioned and especially applicable in the treatment of severely ill patients. However, the degree of sharing with "health care providers" (defined as shown in Table 1) permitted by the proposed amendments is so broad that it fundamentally and radically changes the concepts of consent and confidentiality so as to render them virtually meaningless.

The central provision of the proposed amendment permits mental health information to be shared without a process of active, informed consent regarding patients' private mental health records. Unless patients were informed of the process and the risks, understood what was happening, and took active steps to "opt-out" of allowing their information to be shared, their privacy would be invaded. Any anticipated gain resulting from the ability to use computerized systems to share information among "health care providers" would likely be offset by decreased access to care for potential patients who fear lack of privacy for their personal mental health information.

The "opt-out" provision of the proposed amendment also clashes with the premise underlying the United States Supreme Court *Jaffee v. Redmond* decision in 1996, which established an absolute psychotherapist-patient privilege in federal courts. In establishing this privilege, the Justices explained the rationale for providing mental health "counseling" with a degree of privacy not accorded to general medical treatments. They recognized that effective psychotherapy could not take place without full assurance of confidentiality within the patient-therapist dyad.

Sharing of information with health information exchanges, which would combine information from mental health treatments with data from general medical treatments, could undermine the basis for the psychotherapist-patient privilege. Even if a patient is not in formal psychotherapy, some degree of psychotherapeutic "counseling" and self-revelation is integral to effective treatment of any mental disorder, so that practically all patients come to psychiatric treatment hesitantly, with a very high level of concern about privacy.

Why informed consent must be preserved

Computerized networks are not capable of keeping patient information reliably and totally secure. Given this fact, we can ill afford to add private and sensitive mental health information to these systems. For example, in just the 2 years since the HITECH Act's breach notice law went into effect, which requires the Secretary of Health and Human Services to post a list of breaches of unsecured protected health information affecting 500 or more individuals, nearly 12 million Americans have had the privacy of their health information breached.[5] A particularly alarming breach was recently reported, involving Stanford University Hospital in California, in which patients' private information, placed on a computerized health record system, was improperly made available outside the system for a period of 6 months.[6] Such a security breach in the District of Columbia would have a chilling effect on patients' willingness to seek psychiatric treatment, and to provide information necessary for the treatment if they did seek it.

It was recently reported that the Department of Defense is being sued for $4.9 billion dollars due to an electronic health information privacy breach of 4.9 million records by a Tricare contractor.[7] A similar suit in the District of Columbia would have a devastating effect on the ability of the District of Columbia to provide needed treatment for its citizens. One issue that would inevitably come up in

such a suit is whether the patients had been sufficiently informed about the risks associated with having information placed on a computerized network and whether the patients had actively given consent. It is not clear whether the court would view the "opt out" system recommended in the proposed amendments as meeting these criteria.

Less dramatic but more immediate and potentially highly damaging are the issues involved in controlling the dispersal of information within an electronic health information exchange itself. Regional health information exchanges vary widely.[8,9] Some have centralized data collection systems in which full clinical records are stored and accessed by other entities. In other systems, the information remains in the computers of the entity that gathered it, and the system is more of a clearing house that maintains an index of the patients' identifying data that is used to connect the patient's record to other parts of the system that request it. There are many variations from one region or locality to another.

There are control and consent issues at both ends of the intermediary process—data input and data disclosure to other entities in the system. Access to a patient's personal health information is likely to be limited to other providers who are involved in the patient's care—but once access is gained, the patient's whole information set may be open to them unless the patient can control what is disclosed and to whom. Will the patient really want his psychiatric record available to every physician, allied professional, or facility that has something to do with his health? Under HIPAA, disclosure for payment or health care operations is limited to the minimum necessary information—but there is no such limitation for treatment purposes.

Will a psychiatric patient's basic identifying data in a network index include a diagnosis or a problem list or treatments about which the patient may be sensitive? What will govern which persons or entities will be able to access it and for what purposes, to protect against abuses like employment screening, personal curiosity, or harassment by people who have access to the system? These questions raise issues about when a patient will have the right to exercise informed consent: at the beginning or the end of the chain or both? Will a patient be asked to "opt in" or given the opportunity to "opt out" at the initial point where she tells a doctor or a therapist about what is troubling her? Or will the information silently and automatically be entered into the system and then the patient may (or may not) have to give consent or be given the opportunity to withhold it at the point where another provider requests access to that patient's information? Can permission be limited to certain elements of information but not others? Could the system handle such delimited disclosures? (In other words, can it exercise the thoughtful discretion that should automatically play a part when one doctor talks to another?) And finally, will a practitioner or a health care facility within the system refuse to provide care if a patient "opts out"?[10]

Similar issues to those being raised in the District of Columbia have already begun to arise in other parts of the country. On the national level, HIPAA itself has an "opt-out" system in which permission to disclose protected health information for treatment, payment, and health care operations is assumed unless the patient acts to refuse it. Under the HIPAA Privacy Rule, consent for these communications is assumed if the patient enters medical care. However, as part of required full disclosure about HIPAA's privacy regulations, patients must be informed of these communications and given the opportunity to revoke consent. The physician or health care facility has the option of declining to accept this refusal (in which case the patient has the option of leaving) although once accepted, it must be respected. In any electronic health information system, the patient must still be informed of that option and its risks along with the rest of the HIPAA privacy rule and actively given that choice. That is the nature of *informed* consent.

The relatively weak protection in the HIPAA privacy rules has been supplemented up until now by more stringent protections in the laws of some states, which take precedence over HIPAA because, under HIPAA, stricter state privacy laws prevail. These laws require active "opt-in" informed consent for disclosure of health care information. Examples are laws in the District of Columbia and Ohio, where the author lives. But now, as we see in this case in the District of Columbia, those extra protections are under threat.

HIPAA rules require full protection of psychotherapy notes which are part of but must be kept separate from the rest of the official medical record—so that by law psychotherapy notes cannot be entered into an electronic system if anyone else can access the information in those notes without specific and limited authorization by the patient. However, other

psychiatric and mental health records besides psychotherapy notes can contain highly sensitive and potentially damaging information. The details of a multi-axis DSM-IV diagnosis, prescribed medications (even in the absence of a diagnosis), problem list behavioral data (e.g., suicidal impulses or actions, illegal or embarrassing behavior), elements of past history—all are examples of information patients would not want to be disclosed except possibly to a select, trusted professional who is directly involved in their care at their discretion.

All states have laws protecting the privacy of health care information. Maintaining that requirement is a mark of respect for the patient, and it preserves the privacy, confidentiality, and informed consent that are fundamental to patients' willingness to enter into mental health treatment and to the treatment process itself.

For these reasons, any modification of existing laws protecting privacy and the right of informed consent should be very carefully thought through. There can be great value when information is properly shared among those providing health care to patients. While current systems of obtaining informed consent for disclosure of mental health records may feel cumbersome in comparison to the automated entry of data into an electronic health information exchange system, patients have a right to know 1) that there is a significant risk to privacy and confidentiality in maintaining mental health information in electronic networks and 2) that consent is theirs to give or refuse. A security breach of mental health information in an electronic health exchange in a city like Washington, D.C., could be devastating. The proposed amendments in the District of Columbia would discourage people from seeking treatment, as well as from providing accurate and complete information when they do seek treatment. When information from mental health treatments needs to be shared for optimal patient care, it is crucial that a more focused and less global solution be found that respects the right of individual patients to control disclosure of their personal health information and does not potentially compromise the privacy, confidentiality, and security of mental health records.

References

1. Health IT and patient safety: Building safer systems for better care. Institute of Medicine Nov. 2011 (available at iom.edu/~/media/Files/Report%20Files/2011/Health-IT/HealthITandPatientSafetyreportbrieffinal_new.pdf, accessed January 7, 2012).
2. American Psychiatric Association. Minimum necessary guidelines for third-party payers for psychiatric treatment: Position statement. APA November 2002 (available at www.psych.org/Departments/EDU/Library/APAOfficialDocumentsandRelated/PositionStatements/200211.aspx, accessed December 9, 2011).
3. Mental Health Information and Primary Care Integration Act of 2011 (available at www.scribd.com/doc/60402524/Untitled, accessed December 20, 2011).)
4. District of Columbia Behavioral Health Association. The Mental Health Information & Primary Care Integration Act: Fact sheet, posted August 8, 2011 (The fact sheet has recently been revised and this controversial reference to consent has been removed, although the bill and its intent remain the same. The current version of the fact sheet is available at www.dcbehavioralhealth.org/news/thementalhealthinformationprimarycareintegrationact, accessed January 6, 2012).
5. Department of Health and Human Services, Office of Civil Rights. Breaches affecting over 500 individuals. Information available at www.hhs.gov/ocr/privacy/hipaa /administrative/breachnotificationrule/postedbreaches.html and www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html, accessed December 19, 2011.
6. Sack K. Patient data posted online in major breach of privacy. New York Times, September 8, 2011 (available at www.nytimes.com/2011/09/09/us/09breach.html, accessed December 19, 2011).
7. Vijayan J. Defense Dept. hit with $4.9 B lawsuit over data breach. Computerworld, October 14, 2011 (available at www.computerworld.com/s/article/9220874/Defense_Dept._hit_with_4.9B_lawsuit_over_data_breach, accessed December 31, 2011).
8. Wikipedia. Regional health information organization. Article available at en.wikipedia.org/wiki/Regional_Health_Information_Organization, accessed December 27, 2011).
9. Just B, Durkin S. Clinical data exchange models. Appendix to Acker B, Birnbaum CL, Braden JH, et al. HIM principles in health information exchange. J AHIMA. 2007;78:69–74 (available at library.ahima.org/xpedio/groups/public/documents/ahima/bok1_035093.pdf, accessed December 27, 2011).
10. Neumeister R. My privacy rights negated by "blackmail." Open Secrets Minnesota Blog posted on the Twin Cities Daily Planet, December 25, 2011 (available at www.tcdailyplanet.net/blog/anonymous/my-privacy-rights-negated-blackmail, accessed December 27, 2011).