Dispelling the Myths about Information Sharing Between the Mental Health and Criminal Justice Systems

John Petrila, JD, LLM[1]

The CMHS National GAINS Center for Systemic Change for Justice-Involved People with Mental Illness February, 2007

Recently, police arrested an individual with a long arrest record. During the arrest, he was injured and police took him to an area hospital for care. When the police came to check on him the next day, he had been released. The hospital spokesperson said that the Health Insurance Portability and Accountability Act (HIPAA) made it impossible for the hospital to communicate with the police regarding the individual's release.

This 2006 newspaper story is notable for two reasons. First, it illustrates one of the many types of interactions between law enforcement officials and health care providers that occur every day across the United States. Second, it illustrates the many misunderstandings regarding HIPAA that continue to exist years after its enactment.

These misunderstandings are sometimes so deeply ingrained that they have assumed the status of myth. These myths have serious negative consequences for persons with mental illness who are justice-involved. They can bring efforts at cross-system collaboration to a halt and they can compromise appropriate clinical care and public safety. In fact, these myths are rarely rooted in the actual HIPAA regulation. HIPAA not only does not create a significant barrier to cross-system collaboration, it provides tools that communities should use in structuring information sharing arrangements.

Contrary to myth, HIPAA covered entities do not include the courts, court personnel, accrediting agencies such as JCAHO, and law enforcement officials such as police or probation officers.

What is HIPAA?

Congress enacted HIPAA in 1996 to improve the health care system by "encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information."

The HIPAA "Privacy Rule" (which establishes standards for the privacy of information and took effect on April 14, 2003) has received most of the attention from those concerned about the impact of HIPAA. However, as important, the Department of Health and Human Services adopted the Rule on Security Standards in 2003, to govern the security of individually identifiable health information in electronic form. An Enforcement Rule was also adopted, effective March 2006. Most of the myths about HIPAA concern the Privacy Rule, while too often ignoring the potentially more troublesome area of electronic security.

Who does the HIPAA Privacy Rule cover?

The Privacy Rule establishes standards for the protection and disclosure of health information. The Privacy Rule only applies to "covered entities," which are health plans (such as a group health plan, or Medicaid); health care clearinghouses (entities that process health information into standard data elements); and health care providers. Other entities may be

[1] Department of Mental Health Law & Policy ◆ University of South Florida at Tampa

affected by HIPAA if they are "business associates" (discussed briefly, below).

Contrary to myth, HIPAA-covered entities do *not* include the courts, court personnel, accrediting agencies such as JCAHO, and law enforcement officials such as police or probation officers. There are special rules for correctional facilities, discussed briefly below.

What does the Privacy Rule require before disclosure of protected health information?

The Privacy Rule permits disclosure of health information in many circumstances *without requiring the individual's consent to the disclosure*. These circumstances include the following:

- Disclosures or uses necessary to treatment, payment, or health care operations. This means, for example, that a care provider may release information to another treatment provider at discharge, because the disclosure is necessary for treatment. In addition, "health care operations" is defined broadly and includes quality improvement, case management, and care coordination among other things.

- HIPAA also permits other disclosures without the individual's consent. Those relevant here include disclosures for public health activities; judicial and administrative proceedings; law enforcement purposes; disclosures necessary to avert a serious threat to health or safety; and disclosures mandated under state abuse and neglect laws.

  In the example provided at the beginning of this fact sheet, the hospital properly could have notified law enforcement of the presence of the arrestee in the hospital under the provision of HIPAA that permits a covered entity to disclose protected health information to a law enforcement official's request for "information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person" (164.512(f) (2). While this section limits the type of information that may be disclosed for this purpose, it is clear that identifying information can be disclosed.

- In the case of correctional facilities, HIPAA permits health information to be shared with a correctional institution or law enforcement official with custody of the individual, if the information is necessary for the provision of health care to the individual; the health and safety of the inmate, other inmates, or correctional officials and staff; the health and safety of those providing transportation from one correctional setting to another; for law enforcement on the premises of the correctional facility; and for the administration and maintenance of the safety, security, and good order of the facility. This general provision does not apply when the person is released on parole or probation or otherwise released from custody.

HIPAA not only does not create a significant barrier to cross-system collaboration, it provides tools that communities should use in structuring information sharing arrangements.

Does this mean that consent is never required in these circumstances?

While HIPAA permits disclosure without consent in many situations, it does not mean that unlimited disclosure is permissible or that obtaining consent is unnecessary or inappropriate. First, confidentiality and privacy are important values in health care. Obtaining consent may be a way of demonstrating respect for the individual's autonomy, whether or not it is legally required. Second, other laws may mandate that consent precede disclosure even if HIPAA does not. If a state law provides more stringent protection of privacy than HIPAA, then the state law must be followed. The same is true of the Federal rules

on the confidentiality of alcohol and drug abuse patient records (commonly referred to as Part 2). These rules, enacted more than 30 years ago, have strict requirements for the release of information that would identify a person as an abuser of alcohol or drugs. Another example illustrates this point: HIPAA permits disclosure of information in response to judicial and administrative subpoenas that many state laws limit. If state law has more procedural protection for the individual in that circumstance, then state law applies. Finally, HIPAA incorporates the principle that in general disclosures should be limited to the "minimal necessary" to accomplish the purpose for which disclosure is permitted.

Are there tools that can be used in cross-system information sharing?

There are several tools systems can adopt in creating an integrated approach to information sharing.

- *Uniform consent forms*. While HIPAA does not require prior consent to many disclosures, consent may still be necessary for legal (i.e., other state law) reasons, or because it serves important values. One barrier to collaboration is that most agencies use their own consent forms and consent is obtained transaction by transaction. In response, systems can adopt uniform consent forms that comply with Federal and state law requirements.

  Such forms have several features. First, they permit consent to be obtained for disclosure throughout the system at whatever point the individual encounters the system. Second, the forms can be written to include all major entities in the collaborative system; the individual can be given the option to consent to disclosure to each entity in turn, by checking the box next to that entity, or consent can be presumed with the individual given the option of withholding information from a particular entity.

- *Standard judicial orders*. Courts and court officers (state attorneys, public defenders) are not covered entities under HIPAA. However, in some jurisdictions care providers have been reluctant to share health information with the courts, or with probation officers, on the ground that HIPAA prohibits it. In response, some judges have created judicial orders with standard language mandating the sharing of information with certain entities, for example probation officers. Such orders do not concede that courts or court officers are covered by HIPAA; rather they are designed to eliminate mistaken assumptions that care providers may have regarding HIPAA.

- *Business associate agreements*. A "business associate" is a person or entity that is not a covered entity but that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. Examples include the provision of accounting, legal, or accreditation services; claims processing or management; quality assurance; and utilization review. Entities or persons providing these and other services described in the regulation must sign a business associate agreement with the covered entity for which the services are provided.

HIPAA does not discuss uniform consent forms or standard judicial orders, but it is evident that both will assist in easing sharing of information within and across systems. HIPAA does require the use of business associate agreements in some circumstances, and so knowledge of the requirements for such agreements is important. 42 CFR Part 2, on the confidentiality of alcohol and substance use information, has an analogous though not identical provision permitting the sharing of information with "qualified services organizations."

Will HIPAA violations lead to severe penalties?

The fear of liability far outstrips the actual risk of liability in providing mental health care. This is true generally, and particularly true with confidentiality, where there have been few

lawsuits in the last three decades alleging a breach of confidentiality.

There is also great fear regarding the possibility of punishment for violating HIPAA. Certainly, HIPAA provides for significant penalties, including civil and criminal fines and incarceration. However, there are two reasons that penalties for minor HIPAA violations, in particular, are unlikely. First, if an individual's health information is disclosed inappropriately under HIPAA, that individual cannot bring a lawsuit for the violation. Rather, enforcement of HIPAA is done entirely through regulatory agencies, with primary enforcement the responsibility of the Office of Civil Rights of the Federal Department of Health and Human Services. Second, although, there had been 22,664 complaints received by OCR through September 30, 2006, not a single penalty has been imposed.

... through September 30, 2006, not a single [HIPAA violation] penalty has been imposed.

In fact, only 5,400 (or 23%) complaints required further investigation, and these were resolved either by informal action (for example, a letter) or no further action. Therefore, the actual, as opposed to perceived, risk for being severely punished for a HIPAA violation is remote.

A note on the Rule on Security Standards

As noted above, this rule was adopted in 2003 but has received comparatively little attention in discussions of cross-system collaboration. Yet while concerns regarding the Privacy Rule have been exaggerated in many jurisdictions, security issues may sometimes receive too little attention. For example, while protected health information may be shared in most circumstances, if it is done electronically steps must be taken to secure the information, for example by encrypting email exchanges. As systems get beyond the myths regarding sharing of information under HIPAA, it will be important to focus on the requirement of the Security Standards, particularly since the most egregious violations of individual privacy over the last few years have resulted from intrusions into electronic data.

Summary

HIPAA has become the reason many conversations regarding cross-system collaboration have come to a stop. Yet HIPAA provides no significant barrier to sharing information within and across systems. While confidentiality and privacy of health information are important and legally protected values, HIPAA has become subject to myths that have no foundation in the text of the regulation. It is important that all parties involved in efforts to create integrated systems for people with mental illnesses in the criminal justice system put HIPAA aside as a reason these efforts cannot succeed. ■

Useful Resources

www.hhs.gov/ocr/hipaa

This is the home page for the Office of Civil Rights of the US Department of Health and Human Services. OCR has primary enforcement authority for HIPAA. This page has a wealth of information regarding HIPAA — it's the first place to go with questions.

www.hipaa.samhsa.gov/download2/SAMHSAHIPAAComparisonClearedPDFVersion.pdf

This page links to a document prepared by SAMHSA that compares Part 2 (the Federal regulations on the confidentiality of substance use and alcohol information) with the HIPAA Privacy Rule.

www.hhs.gov/ocr/combinedregtext.pdf

This link provides the full text of the Privacy Rule and Security Standards for the Protection of Electronic Protected Health Information.

www.gainscenter.samhsa.gov/html/resources/presentations.asp

This page includes an audio replay and materials from a CMHS TAPA Center for Jail Diversion net/tele-conference: *HIPAA and Information Sharing*. A sample uniform consent form is included.