Justice and Health CONNECT
A national resource for justice and health data sharing

The Legal Landscape of Justice and Health Information Sharing

Policymakers interested in exploring information-sharing arrangements between health and justice agencies frequently cite laws protecting personal health information as a barrier to engaging in cross-system data sharing. Medical privacy laws can be especially stringent when disclosing information on mental health, substance use, and communicable diseases such as HIV/AIDS. In fact, some federal courts have recognized a constitutional right to medical privacy in this domain. These federal, state, and local laws, rules, and regulations provide necessary protections of individual privacy and confidentiality, but they should not be seen as insurmountable obstacles to cross-agency information sharing. In most cases, it is possible to share information to improve access to treatment, with the necessary permissions and if safeguards are established to shield sensitive health information from unwarranted disclosures. There are a number of detailed guidelines describing privacy regulations and examples of jurisdictions that have successfully established justice and health information exchanges listed in the Justice and Health Connect resource library.

A number of federal regulations apply nationally (including 42 CFR, Part 2 and HIPAA, mentioned below) and in most jurisdictions there are state and local laws that place additional conditions on the use and disclosure of confidential health information. Policymakers considering information sharing arrangements should first conduct a legal analysis of federal, state, and local laws, regulations and policies that govern the transmission of personal health information in their jurisdiction. When conducting a legal analysis, it is important to determine (1) which laws apply based on the type of information you want to share; (2) whether the law applies to the agency or person releasing information; (3) whether the law applies to the agency or person requesting information; and (4) what the law requires in terms of consent processes and data security based on the problem you are trying to address and what you intend to accomplish with data sharing.

The Laws you Need to Know

> **Constitutional right to medical privacy.** Certain federal and state courts recognize a constitutional right to medical privacy under the 14th Amendment.[1] This right has been recognized specifically in the context of protecting confidentiality and harmful disclosures of sensitive health information in correctional settings.

[1] For example, see *Doe v. Delie*, 257 F.3d 309 (3rd Cir. 2000) (recognizing prisoner's 14th Amendment right to medical privacy, which was violated by open-door exam policy, disclosure of condition to correctional escorts, loud announcement of medications); *King v. State*, 535 S.E.2d 492 (Ga.,2000) (Medical records are within the right of privacy afforded by the Federal Constitution); *Powell v. Shriver*, 175 F.3d 107, (9th Cir. 1999) (HIV and gender identity disorder); *O'Connor v. Pierson*, 426 F.3d 187 (2d Cir. 2005) (psychiatric disorder and substance abuse

- **The Health Insurance Portability and Accountability Act (HIPAA).** HIPAA establishes national standards for the privacy and security of an individual's protected health information (PHI) that is created, used, or maintained by a "covered entity" or their business associates. Protected health information is any information about health status, provision of health care, or payment for health care that can be linked to a specific individual.

  Covered entities include health plans, health care clearinghouses, and health care providers that transmit health information electronically. While HIPAA makes it clear that some criminal justice entities are not "covered entities" and thus not required to obtain prior authorization before communicating health information (e.g. law enforcement, courts and probation), the definition of "covered entity" has been ambiguously interpreted by jails, prisons, and pretrial services because their primary purpose is not to provide or pay for health services. Though HIPAA permits community health providers to share health information with criminal justice agencies, without an individual's consent, when they have "lawful custody" of that individual and the information is needed to promote continuity of care and safety. [2] It is important to know when HIPAA requires informed consent/authorization prior to transmitting PHI, as well exceptions to these requirements. For a concise explanation of these exceptions, see *Dispelling Myths about Information Sharing between the Mental Health and Criminal Justice Systems* by Professor John Petrila and the National GAINS Center.

- **42 CFR, Part 2.** 42 CFR, Part 2 limits entities receiving federal assistance from the disclosure and use of information that could be used to identify a patient as having or seeking treatment for an alcohol or substance use problem.[3] The regulations stringently preclude accessing substance use treatment information for purposes of criminal prosecution. In most scenarios, before treatment information can be released, Part 2 requires the informed consent of the patient. Moreover, even when a valid consent process permits certain parties in the justice system to receive substance use treatment information (for example, as a condition to criminal disposition), Part 2 places firm requirements on the individuals and entities that are able to access records. Specifically, the regulations place limits on the use of information to an explicitly confirmed purpose, and specify the duration of consent.

- **State Laws: Medical Privacy, Informed Consent, Clinician-Patient Privilege.** An understanding of state law is essential because both HIPAA and 42 CFR Part 2 have exemptions from their preemption clauses, allowing state law to govern if it is more protective or restrictive than the federal standards.[4] State laws vary in terms of their complexity, certainty, and applicability to different types of protected health information. For instance, the definitions of 'informed', 'knowing', and voluntary consent requirements to disclose personal health information are subject to considerable state-by-state variation.

---

[2] See, Orr, D. and Hellerstein, *HIPAA in State Correctional Institutions*, Journal of Correctional Health Care, 2002.
[3] Federal assistance includes, but is not limited to, entities that receive funding from the federal government, organizations with 501c nonprofit status, programs that accept Medicaid reimbursements, facilities that are licensed by federal agencies, tax exempt programs, and programs that offer income-tax deduction to funders or supporters.
[4] *See* 46 C.F.R. § 160.203; *See* 42 C.F.R. § 2.20.

Practitioners should seek the advice of local, county, or state counsel to determine whether federal or state law is more restrictive in a given area.

- **Local Rules and Regulations.** Institutions typically have their own policies governing data and personal information, which should also be consulted. For example, many accrediting agencies for hospitals and most state licensing agencies maintain strict requirements regarding treatment record confidentiality and require facilities to comply with HIPAA and 42 CFR, Part 2.

- **Privacy Principles and Fair Information Practice Principles.** These principles thread throughout privacy law, describing the appropriate balance between confidentiality, trust, accountability, autonomy, and public interest in disclosure. The Fair Information Practice Principles include the data quality principle, use limitation principle, and individual participation principle. For more information on these principles and their application in justice and health settings see the OECD Privacy Principles and The Fair Information Practice Principles.

Addressing Legal Restrictions on Information Sharing

Once policymakers and practitioners understand the legal landscape at the federal, state and local level, including which laws apply to them or the agencies they hope to work with, the next step is to determine which tool(s) will best enable them to work within the laws in order to legally and ethically share information. These include the use of client consents to share personal information, data segmentation, data sharing agreements, new legislation, and executive orders.

- **Informed Consent.** Most of the regulations listed above allow PHI to be shared with the informed consent of the individual involved. Drafting forms that document the provision of individual consent to share personal information and developing procedures to authorize release of PHI are one way to facilitate data exchanges. Informed consent forms are routinely used by healthcare providers to allow information sharing necessary to provide medical care in a range of settings. Agencies have developed single or multi-party consent forms to enable communication between stakeholders coordinating care and services, while respecting autonomy and privacy of the patient. For example, Riverside County, California uses a single authorization form to allow mental health staff to share information with public defenders' and district attorneys' offices, probation officers, and any contracting agencies that may be involved with providing services to people participating in the Riverside County mental health court.[5] Practitioners should ensure that the language on consent forms complies with the appropriate federal and state legal requirements. For examples of single and multi-party consent forms used in a range of settings, see the Justice and Health Connect Resource Library.

[5] John Petrila et al., *Information Sharing in Criminal Justice-Mental Health Collaborations: Working with HIPAA and Other Privacy Laws*, (New York: Council of State Governments, 2010).

- **Data Segmentation.** This process limits what can be viewed in a person's medical record and allows for access to vary depending on the recipient agency. Data segmentation can be used to allow information to be shared in specific instances that are permissible under information sharing regulations. For example, segmentation can be used to allow entities directly involved in treatment to share diagnostic and clinical information, while restricting access for others with administrative roles to the minimum amount of information necessary. Segmentation can also allow patients to play an active role in determining which portions of their records can be exchanged and which providers within a network can have access.

- **Memorandum of Understanding (MOUs).** MOUs can be used to set the parameters and specifications of an information sharing agreement between agencies. These contracts can help solidify interagency collaborations by defining responsibilities, explicitly documenting the intended purpose of data sharing, and specifying a planned course of action for any breaches.

- **State Legislation.** State legislation can be used to authorize information sharing between criminal justice and health systems for certain purposes. For example, legislation in Illinois supported the Illinois Jail Data Link by allowing county jails to have access to an internet database which provided data on detainees with documented mental illness and treatment with the Division of Mental Health.[6]

- **Executive Orders.** Executive orders can provide the authority required to create an information sharing system. Typically, executive orders establish a statement of purpose for the information sharing system and transparency and accountability mechanisms to ensure compliance with all applicable laws. For example, New York City's HHS Connect is supported by an executive order from the Mayor's office to facilitate electronic data exchange between the Administration for Children's Services, Department for the Aging, Department of Correction, Department of Health and Mental Hygiene, Department of Homeless Services, Department of Juvenile Justice, Department of Probation, Health and Hospitals Corporation, and Human Resources Administration.

[6] *Ibid*

Important Resources

Goldstein, Melissa. *Health Information Privacy in the Correctional Context*. COCHS Conference on Health Reform and Criminal Justice: Integrating Jails into Health Information Exchanges. Community Oriented Correctional Health Services, April 3, 2012.

Petrila, John. *Dispelling the Myths about Information Sharing Between the Mental Health and Criminal Justice Systems.* Delmar, NY: Policy Research Associates and CMHS National GAINS Center, 2007.

Petrila, John, et al. *Information Sharing in Criminal Justice-Mental Health Collaborations: Working with HIPAA and Other Privacy Laws.* New York: Council of State Governments, 2010.

Beckerman, Julia Z., et al. "Health Information Privacy, Patient Safety and Health Care Quality: Issues and Challenges in the Context of Treatment for Mental Health and Substance Use." Health Care Policy, 16, 2 (2008).

Marks, PD. "Reaching a balance between privacy, privilege, and planning: A look at the barriers to obtaining information for patients with criminal involvement." Psychiatric Quarterly, 75, 2 (2004), 127-38.

U.S. Department of Health and Human Services. "Understanding Health Information Privacy." http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html.

The Substance Abuse and Mental Health Service Administration (SAMHSA). "Applying the Substance Abuse Confidentiality Regulations to Health Information Exchange." http://www.samhsa.gov/healthprivacy/docs/ehr-faqs.pdf.