Health Information Privacy in the Correctional Environment

By Melissa M. Goldstein, JD, The George Washington University

Information technology is considered a transformative element in health care because it facilitates the transparency and sharing of health information, which have always been central to the practice of medicine and the delivery of high quality care.[1] The widespread use of electronic health records (EHRs) and electronic health information exchange, among other technologies, is considered essential to improving the quality of care, reducing medical errors, reducing health disparities, and advancing the delivery of patient-centered medical care.

While it is widely acknowledged that information about patients and their health needs to go where it is needed, when it is needed, and be accessible to those who can use it to make important treatment and other patient care decisions, it is also recognized that appropriate privacy and security policies must be established and enforced if we truly are to achieve the benefits of electronic exchange.[2] Nationwide polls show that Americans continue to be deeply concerned about the privacy and security of their health information, particularly when it is in electronic form,[3] illustrating our ongoing challenge of balancing society's need to improve the quality, safety, and efficiency of health care with the protection of personal health information.

This balance becomes relevant in the U.S. correctional setting because of the high numbers of Americans affected: the Pew Center of the States reported in 2008 that more than 2.3 million people are behind bars on any given day—more than 1 in 99 Americans.[4] With regard to the jail population in particular, local jails admitted an estimated 12.9 million people during the 12 months ending June 30, 2010, with a midyear inmate population of 748,728.[5]

COCHS
COMMUNITY ORIENTED CORRECTIONAL HEALTH SERVICES

This population is also disproportionately ill, with high rates of health problems (e.g., chronic and infectious disease, injuries), psychiatric disorders, and substance use disorders.[6] For example, jail inmates have been found to have a higher prevalence of hypertension, diabetes, myocardial infarction, asthma, arthritis, cervical cancer, and hepatitis than non-institutionalized adults.[7] In addition, prevalence rates of serious mental illness for recently booked jail inmates have been estimated at 14.5% for males and 31% for females (16.6% overall),[8] while over two-thirds (68%) of jail inmates meet DSM-IV criteria for substance abuse or dependence.[9]

This population is often at its sickest when detained, frequently experiencing a psychiatric crisis and/or active addiction. In fact, 80% of detained individuals with a chronic medical condition have not received treatment in the community prior to arrest.[10] Jail inmates' health information may originate from and/or reside in multiple and varied locations within a jail system, including booking notes (e.g., infectious/chronic disease status), a sick-call triage system, physician notes, as well other departments, such as housing and work details.

The use of health information technology (IT) in correctional systems appears to be quite limited at the present time, however. While research on the issue is scarce, one recent study found a wide range of technological sophistication among prison facilities with rare use of EHRs, for example, which affected the institutions' ability to collect performance measurement data.[11] In addition, there appears to be very little to no electronic exchange of health information within systems or between correctional systems and providers in the community. There are signs, though, that EHR use is increasing in these systems. For example, the Texas Department of Criminal Justice's adoption of an EHR system that tracks medical, dental, mental health, and pharmacy services at 120 state prisons, three federal prisons, 15 youth prisons, and county jails reportedly reduced state spending by about $1 billion over the past decade in combination with increased use of telemedicine.[12] Other systems apparently have begun

using EHRs as well, including the Georgia Department of Corrections,[13] the Philadelphia Prison System,[14] the Maricopa County, Arizona jails,[15] and the Los Angeles County juvenile detention facilities.[16]

This article describes the legal environment in which health information-sharing occurs in correctional settings during this era of scant but increasing use of health IT, but is not intended to be a comprehensive legal review. Numerous and varied state and federal laws form the structure of this environment, but it is beyond the scope of this paper to review all of those laws. Instead, select individual statutes and regulations will be examined that apply to health information generally and/or to specific health conditions or types of information that are considered sensitive and therefore protected by legislation.

As discussed below, the overarching purpose of these state and federal laws—encouraging and enhancing patient participation in the health care system—is sometimes modified in practice in the correctional environment. It should be noted as well that their application will vary depending on the particular correctional institution and location involved—that is, whether an institution is a county jail or a federal prison, the ways in which it delivers health care to its inmates, and/or what state it is located in might affect the determination of any particular legal question. Local institutional policies and practices as well as local, county, or state counsel should always be consulted in making such determinations.

Health information privacy law

Privacy laws have been described as supporting the expression of patient preferences regarding the sharing of personal health information, thereby supporting underlying principles of personal autonomy and encouraging patient engagement. In the context of bioethics, personal autonomy is the principle on which an individual patient's right to make and carry out informed decisions regarding his or her health is based, including decisions regarding access to personal health information.[17] Autonomy has been described as "the accepted rationale" for ensuring the confidentiality and privacy of health information,[18] and there is considerable justification for basing policies regarding consent to the sharing of one's health information on the principle of autonomous decision-making.[19]

Professional standards in the correctional context reinforce these principles. The National Commission on Correctional Health Care's *Standards for Health Services in Jails*, for example, states that discussion of patient information and clinical encounters should be conducted in private and "carried out in a manner designed to encourage the patient's subsequent use of health services," which is intended to protect patients' dignity and "foster necessary and candid conversation between patient and health care professional."[20] The Commission further recommends that: "Local, state, or federal laws may allow certain exceptions to the obligations of health care professionals to maintain confidentiality; health services staff should inform inmates at the beginning of the health care encounter when these circumstances apply."[21] The American Public Health Association (APHA) has also addressed the confidentiality of prisoners' health information, stating that "[p]risoner-patients should be provided the same privacy of health care information as patients in the community."[22] These principles hold especially true in the psychiatric context, where inmates' concern about confidentiality and lack of trust in staff have been identified as factors that prevent them from seeking mental health care.[23]

The ability to achieve true autonomous decision-making in the correctional context has been questioned, however, due to the potential for coercion in such settings, which by nature constrain the freedom of the incarcerated. Moreover, the comprehension capacity among the population involved is often diminished due to low literacy, mental illness, and substance abuse, among other factors.[24] For example, the District of Columbia Department of Corrections (DOC) reports the self-declared education levels of male inmates as 38.9% with no education; 26.6% who have attended and/or completed high school; and 25.5% who began and/or completed their G.E.D. For females, 14.2% have no education; 16.2% have attended and/or completed high school; and 3.8% have begun and/or completed their G.E.D. (64.2% of female inmates did not specify their education level).[25]

Patient decisions to share personal health information, inmate or otherwise, must always be informed, knowing, and voluntary in order to be valid; this does not mean, however, that waivers of confidentiality are invalid simply because they are made in a potentially coercive environment or the individual's other options are unappealing. For example, a participant's consent to disclosure of personal health information is not inherently invalid simply because the consent is a condition of drug court participation and the participant faces a substantial prison sentence if he/ she does not enroll in the program.[26]

Health information privacy law, like all law, continues to evolve. Although the U.S. Constitution does not expressly provide a right to information privacy, the U.S. Supreme Court has recognized a limited Constitutional right to privacy with respect to information held in government databases. Attempts to assert that right more broadly have met with inconsistent results, however, leaving the question of Constitutional protection of health information privacy unresolved.[27] In the correctional context, a number of federal courts have explored the issue of whether the Constitution protects the privacy of inmate medical records, also with inconsistent results. The few that have found a right to privacy in medical records have held that the right must give way when the state has a legitimate penological interest in accessing those records, such as the reporting of medical findings in the ordinary course of prison medical care operations or to prison and jail executives with a reason to know.[28] The "[c]asual, unjustified dissemination of confidential medical information to non-medical staff and other prisoners" and "gratuitous disclosure of an inmate's confidential medical information as humor or gossip," however, are not reasonably related to a legitimate penological interest and have therefore been held unconstitutional.[29]

With respect to protecting the confidentiality of sensitive health information, federal and state privacy laws have long been used to address the stigma and social hostility associated with particular health issues.[30] While there is variation in the requirements and application of these laws, they generally limit the exchange of certain health information without patient consent, at times quite stringently and explicitly. For example, the federal Confidentiality of Alcohol and Drug Abuse Patient Records laws (known as "Part 2"), discussed below, strictly limit the disclosure and use of information regarding individuals in federally assisted alcohol or drug abuse treatment programs, protecting any information that could reasonably be used to identify an individual seeking or obtaining education or treatment.[31] The underlying purpose of such laws and regulations is generally to encourage greater participation and trust in the health care system through protection of a patient's most personal and private health information, thus addressing a possible disincentive for seeking services.[32] However, the patchwork of laws regarding sensitive health information in health records has also been criticized as both inconsistent and incomplete, making interpretation challenging, particularly for those initiating electronic exchange.

The Health Insurance Portability and Accountability Act of 1996

A. Elements of the Privacy Rule

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), which provides for the promulgation of privacy regulations (the HIPAA Privacy Rule)[33] is the key federal law that shapes the legal environment underlying health information-sharing in correctional contexts. HIPAA provides a baseline standard of privacy protection for health information—federal and state laws that offer more stringent privacy protections are not superseded by the Privacy Rule.[34] As described above, there is a considerable body of privacy law at the state level,[35] particularly laws that define and protect certain types of sensitive health information. Most states, for example, have laws addressing information in health records related to HIV status, mental health conditions and substance abuse.[36] As a result, a correctional institution's decisions regarding health information-sharing will likely be affected by state privacy laws and should involve consultation with local, county, or state counsel. For example, HIPAA permits disclosure of information in response to judicial and administrative subpoenas that

state law may limit. If state law has more procedural protection for an individual in that circumstance, then state law might apply.[37]

The HIPAA Privacy Rule governs the use and disclosure of protected health information (PHI) by "covered entities," defined as health plans, health care clearinghouses, and health care providers who transmit health information in electronic form in connection with a covered transaction, such as submitting a health care claim to a health plan.[38] PHI is defined as "individually identifiable health information" that is held or transmitted by a covered entity in any form, including electronic, paper, and oral media, subject to certain limited exceptions (such as the exclusion of employment records).[39]

Pursuant to the Privacy Rule, covered entities may not use or disclose PHI except as permitted or required.[40] Covered entities are generally required to provide a patient's own PHI to the patient or to the patient's representative (see below for exception applied to inmates), and must disclose PHI as requested by the Secretary of the U.S. Department of Health and Human Services (DHHS) for audit or other enforcement purposes.[41] All other potential disclosures, including those that may be required by other federal or state laws, are considered "permitted," that is, allowed under the Privacy Rule.[42] In addition, covered entities are generally required by HIPAA to develop public privacy policies stating when and under what circumstances they disclose PHI,[43] and to take reasonable steps to limit the use or disclosure of and requests for PHI to the minimum necessary to accomplish the intended purpose.[44] This "minimum necessary" requirement does not apply to disclosures to or requests by a health care provider for treatment purposes, or to disclosures to the individual who is the subject of the information.[45]

The Privacy Rule requires an "authorization" for uses and disclosures of PHI not otherwise permitted or required,[46] which is a detailed document that gives covered entities permission to use PHI for specified purposes. The elements of a valid authorization are stringent, requiring, for example, a description of the PHI to be used and disclosed, the person authorized to make the use or disclosure, the person to whom the covered entity may make the disclosure, an expiration date, and, in some cases, the purpose for which the information may be used or disclosed.[47]

The Privacy Rule permits covered entities to use and disclose PHI without written patient authorization for purposes related to treatment, payment, and health care operations.[48] HIPAA also permits, but does not require, a covered entity to seek patient *consent* for uses and disclosures of PHI for those purposes, but does not explicitly define consent or specify the necessary content of a consent form or the process by which an entity should obtain consent. DHHS guidance, however, defines the term as written permission from individuals to use and disclose their PHI for treatment, payment, and health care operations.[49] Other uses and disclosures permitted without patient authorization include, for example, disclosures for judicial and administrative proceedings,[50] for law enforcement purposes,[51] to avert a serious threat to health or safety,[52] and for correctional institutions and other law enforcement custodial situations, discussed in more detail below.[53] When the Privacy Rule requires an authorization, voluntary consent is not sufficient to permit a use or disclosure of PHI.[54] In most cases, a covered entity may not withhold treatment or payment if a patient declines to authorize the particular use or disclosure.[55]

The Health Information Technology for Economic and Clinical Health (HITECH) Act recently amended HIPAA by expanding its reach, strengthening certain aspects of the regulations, and increasing federal enforcement tools.[56] For example, because HIPAA has applied only to covered entities, some of the new entities being created to store, handle, or manage electronic personal health information, such as health record banks, have not been directly covered by the Privacy Rule.[57] HITECH has clarified that organizations that provide data transmission of PHI to a covered entity (or its business associate) and require routine access to PHI are business associates as contemplated by HIPAA and must enter into business associate contracts with the covered entity.[58] In addition, HITECH provides that certain provisions of the HIPAA Privacy and Security Rules will be directly applicable

to business associates (in contrast to previous HIPAA requirements, in which business associates were only governed by business associates agreements).[59] The privacy and security requirements created by HITECH itself will apply directly to business associates, and business associates will now be subject to the same civil and criminal penalties applicable to covered entities under HIPAA.[60] Finally, HITECH strengthens HIPAA privacy enforcement by including new enforcement approaches, applying tiered penalties based upon the nature and extent of a violation and the harm caused, and empowering state attorneys general to bring civil suits in federal court to recover damages on behalf of their states' citizens.[61] Regulations implementing the law's provisions are currently being promulgated.

B. HIPAA in the correctional context

In response to the initial version of the Privacy Rule, which would have excluded the individually identifiable health information of correctional facility inmates from the definition of PHI because "unimpeded sharing of inmate identifiable health information is crucial for correctional and detention facility operations,"[62] DHHS received many, ultimately persuasive, comments arguing that excluding such information from protection sends the message that, with respect to this population, abuses do not matter. Commenters argued that, on the contrary, inmates have a right to privacy in their health information and that information obtained in these settings can be misused. For example, if used indiscriminately, health information could trigger assaults within correctional facilities on individuals with stigmatized conditions by fellow inmates; lead to the denial of privileges; and inappropriately influence the deliberations of bodies such as parole boards. Upon release, such disclosures could seriously impair individuals' reintegration into society and subject them to discrimination as they seek community acceptance. These concerns were noted particularly with respect to individuals (especially juveniles) with serious mental illness, seizure disorders, and emotional or substance abuse disorders. Commenters argued that disclosing the fact that such individuals were treated for mental illness while incarcerated could not only impair the individual's reintegration into the community, but could also put the individual or family members at risk of discrimination by employers and in the community at large. The drafters of the final regulation were persuaded by these arguments and eliminated the exception.[63]

a. Status as a covered entity

As discussed above, the Privacy Rule applies only to the use and disclosure of PHI by covered entities. For this reason, correctional institutions should first assess whether or not they are covered entities in order to determine whether they must comply with HIPAA. Unfortunately, this determination has proved vexing for many institutions, and requires careful analysis of the individual institution's operations in collaboration with counsel.

While this analysis will be highly fact-intensive and specific to the individual institution, correctional institutions generally do not process, or facilitate the processing of, health information, and their principal purpose is not providing or paying for the cost of health care. Guidance produced by the Centers for Medicare and Medicaid Services indicates that such institutions therefore are not health care clearinghouses or health plans within the meaning of the Rule.[64] A correctional institution's status as a covered entity would then depend solely on its qualification (or lack thereof) as a health care provider who transmits health information in electronic form in connection with a covered transaction. That is, if the organization "furnishes, bills, or is paid for health care in the normal course of business"[65] and transmits information in electronic form in connection with one of the following eight types of transactions, it is a covered entity and must comply with HIPAA: health care claims or equivalent encounter information; eligibility for a health plan; referral certification and authorization; health care claim status; enrollment and disenrollment in a health plan; health care payment and remittance advice; health plan premium payments; and coordination of benefits.[66]

Although correctional institutions are not likely to engage in most of the transaction types specified by the regulations, it is conceivable that one might transmit clinical encounter information for the purpose of reporting health care; request review of health care in order to secure an authorization; and/or receive payment of

health care claims from a private or public health plan. If the correctional institution electronically transmits one of these transactions or has a contract with another provider who transmits the health care information electronically, it will be required to comply with HIPAA. Correctional institutions must comply with HIPAA even if they contract out the relevant health care services.[67]

Accordingly, some analysts have concluded that state and county departments of corrections as well as local jails must comply with HIPAA if they bill electronically for inmate health care. If county departments of corrections have agreements with local hospitals or medical centers to provide inmate health care and those providers bill the department of corrections electronically, the department likely will be required to comply with the Privacy Rule. Likewise, an institutional health clinic, a social worker or psychologist, and a county hospital that provides health services to inmates would all qualify as covered health care providers if they directly work for or electronically bill the correctional institution.[68] On the other hand, if a correction institution is self-insured and self-pays and does not engage in standard transactions, it might be exempted from covered entity status. This could also be the case if an institution has a contract with a third party to provide health care, but participates in no billing using the electronic standards.[69]

Beyond the covered entity question, the Privacy Rule does apply to many community health care organizations, such as hospitals, and will for this reason alone have an impact on correctional providers and their ability to obtain health information.[70] Within the criminal justice context, however, certain stakeholders clearly are *not* covered entities. For example, law enforcement officials are not bound by HIPAA when asked to provide PHI to others except in certain limited circumstances (e.g., pursuant to a protective court order). Nor are probation and parole officers covered entities under HIPAA—for a supervising officer to receive PHI, the individual must give permission or a court must include a provision in the conditions of release that permit the supervising officer to obtain health information when necessary to monitor compliance. Further, HIPAA does not prohibit re-disclosure of PHI by a non-covered entity. That is, if a former inmate discloses PHI to his/her probation officer, the officer may share or re-disclose the information without adhering to the requirements of the Privacy Rule. In both cases, however, state law might place restrictions on the disclosure of PHI.[71]

b. Permitted uses and disclosures

As noted above, the final version of the Privacy Rule considers the individually identifiable health information of prisoners to be PHI to the extent that it otherwise meets the definition and is maintained or transmitted by a covered entity.[72] However, the drafters of the Rule also recognized that correctional facilities have legitimate needs for the use and sharing of inmates' PHI without obtaining authorization.[73] For this reason, the Rule includes special provisions regarding both the permissible uses and disclosures of the PHI of inmates and their ability to exercise the rights otherwise granted in the Rule.

First, the Rule permits a covered entity to disclose inmates' PHI without individual consent, authorization, or agreement to correctional institutions[74] or law enforcement officials having lawful custody of an inmate for specified health care and other custodial purposes. In such a situation, the correctional institution or law enforcement official must represent that the PHI is necessary for one of the circumstances listed in the Rule. It is important to note, however, that while the Privacy Rule might *permit* disclosures without authorization in such circumstances, such disclosures are *not* required by the Rule; that is, a covered entity could choose not to disclose the information at issue or to seek the individual's authorization to do so.

Specifically, covered entities are permitted to disclose PHI to a correctional institution or a law enforcement official having lawful custody of an inmate for the purpose of providing health care to the individual who is the inmate, or for the health and safety of the inmate, other inmates, the officers and employees of and others at the facility, and persons responsible for transporting inmates or their transfer from one institution to another. In addition, a covered entity may disclose PHI as necessary for law enforcement on the premises of the correctional institution and for the administration and maintenance of the

safety, security, and good order of the institution. For example, an institution's triage nurse could disclose the nature of an inmate's injuries from an assault by fellow inmates to correctional officials, since the disclosure could assist in the institution's administrative or criminal investigation and might relate to protecting the safety of the inmate. An institution's health clinic might also properly notify officials of an inmate's HIV status without violating HIPAA, depending on the particular circumstances involved and state law.[75]

These disclosure rules, however, do not apply to release of the PHI of former inmates, or to individuals in pretrial release, probation, or on parole, as such persons are no longer in lawful custody.[76] When individuals are released from correctional facilities, they have the same privacy rights under the Rule that apply to all other individuals, and covered entities must apply privacy protections to their PHI in the same manner and to the same extent that they protect the PHI of others. Further, these rules apply equally to *all* covered entities, including those that are health care components of a correctional institution (such as a prison clinic), and those that provide services to inmates under contract to correctional institutions.[77]

Beyond this exception, the Privacy Rule also permits a range of other uses and disclosures of PHI without individual consent, authorization, or agreement that are relevant to criminal justice activities, although the scope of this article does not allow for detailed descriptions of all of these situations. Such permitted disclosures include those related to public health activities;[78] judicial and administrative proceedings;[79] certain law enforcement purposes;[80] those necessary to avert a serious threat to health or safety;[81] to report potential abuse, neglect, or domestic violence to government authorities;[82] and disclosures required by law.[83] In all of these scenarios, the Privacy Rule *permits* the disclosures in question within certain parameters, but does not require them. Covered entities are always free to seek the individual's authorization, or to choose not to disclose the information. However, while the Privacy Rule itself may not require a particular disclosure, a covered entity might face repercussions for failing to comply with other laws or requirements (such as child abuse reporting laws or in the case of a court order). Moreover, if state law provides more protection for the information concerned in any particular circumstance, then state law applies.

In the law enforcement context, for example, a covered entity is permitted to disclose limited, specified PHI without prior authorization in response to a law enforcement official's request for the information for the purpose of identifying or locating a suspect, fugitive, material witness or missing person.[84] In addition, the Rule allows a covered entity to use or disclose PHI without authorization if the covered entity believes, in good faith, that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat.[85] In the context of a judicial or administrative proceeding, a covered entity may disclose PHI without authorization in response to an order of a court or administrative tribunal, provided that the covered entity only discloses the PHI expressly authorized by the order. In the absence of a court order, a covered entity may disclose PHI in response to a subpoena, discovery request, or other lawful process if the covered entity receives satisfactory assurance from the party seeking the information that reasonable efforts have been made to give notice of the request to the individual who is the subject of the PHI or that reasonable efforts have been made to attain a qualified protective order for the PHI.[86]

c. Additional HIPAA provisions specific to inmates

The Privacy Rule also includes special provisions regarding the ability of inmates to exercise the rights otherwise granted in the Rule. First, the Rule provides a general right for individuals to receive adequate notice of the uses and disclosures of PHI that a covered entity may make and of the individual's rights and the covered entity's legal duties with respect to PHI. Inmates, however, are expressly excepted from this right to notice and, moreover, the requirement does not apply at all to a correctional institution that is a covered entity.[87] Indeed, the drafters of the Rule specifically clarified that "[n]o person, including a current or former inmate, has the right to notice of such a covered entity's privacy practices."[88]

Thus, present inmates have no right to receive a notice with respect to PHI created during incarceration, and a correctional institution is not required to send a notice to an inmate after release. However, the absence of an affirmative right on the part of an inmate and/or a duty on the part of a correctional institution does not mean that the Privacy Rule forbids a correctional institution from providing inmates with notice under appropriate circumstances. Correctional institutions, and covered entities in general, are always allowed to engage in more privacy-protective practices than required by HIPAA—the Privacy Rule provides only a floor of required protections. As noted above, the National Commission on Correctional Health Care encourages institutions to go above and beyond the requirements of the law by informing inmates at the beginning of health care encounters when local, state, or federal laws allow exceptions to the general obligations of health care professionals to maintain confidentiality.[89]

The Privacy Rule also specifically exempts inmates from the general standard that an individual has a right of access to inspect and obtain a copy of PHI about the individual. In the case of inmates, a covered entity that is a correctional institution or a covered health care provider that is acting under the direction of a correctional institution may deny a request to obtain a copy of PHI, if obtaining the copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for transporting the inmate.[90] However, this ground for denial is restricted to an inmate's request to obtain a *copy* of PHI; if an inmate requests *inspection* of the PHI, the request must be granted unless one of the Rule's other grounds for denial applies (for example, if the records contain information compiled by the institution in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding). As explained by the drafters of the Rule, the purpose for the exception, and the reason that the exception is limited to denying an inmate a copy of the PHI, is to "give correctional institutions the ability to maintain order in these facilities and among inmates without denying an inmate the right to review his or her protected health information."[91] Inmates also retain the right provided by the Rule of requesting amendments to PHI and records in a designated record set, subject to the exceptions provided in the Rule.[92]

Confidentiality of Alcohol and Drug Abuse Patient Records (Part 2)[93]

A. Elements of Part 2

Congress passed legislation in the early 1970s intended to encourage individuals to seek treatment for substance abuse. The statutes and the regulations promulgated thereunder include provisions that protect the confidentiality of persons who seek or obtain substance abuse education or treatment in federally assisted alcohol or drug abuse treatment programs.[94] These laws were intended to assure individuals that information related to substance abuse treatment would be kept private, recognizing that without such assurances, many patients would choose not to seek treatment.[95] According to experts, patient trust in the confidentiality of services is critical in order to enlist patients in treatment programs.[96] The regulations, known as "Part 2," therefore strictly limit disclosure and use of information about individuals seeking or obtaining diagnosis, referral, or treatment in federally assisted alcohol or drug abuse treatment programs.[97] Any and all information that might reasonably be used to identify an individual is protected by Part 2, and all permissible disclosures are limited to the information necessary to carry out the purpose of the disclosure.[98] The regulations do not protect a patient's identity *per se*, but rather his or her identity as a participant in or applicant for substance abuse treatment.[99]

Part 2 defines "disclosure" as a communication or verification of an individual's patient-identifying information, which can include names, addresses, Social Security numbers, fingerprints, photographs, or similar information by which the identity of a patient can be determined.[100] The regulations' requirements apply only to federally assisted programs,[101] defined as individuals or entities that hold themselves out and actually provide alcohol or drug abuse diagnosis, treatment, or referral for treatment, as well as to medical personnel or staff whose primary function is the provision of alcohol or drug

abuse diagnosis, treatment, or referral for treatment.[102] The regulations therefore apply both to freestanding programs and programs that are part of larger organizations, such as a detoxification unit in a county hospital, or a substance abuse clinic in a county mental health department or county jail.[103] "Diagnosis" includes any reference to an individual's alcohol or drug abuse or to a condition that is identified as having been caused by that abuse,[104] including a psychological or social work assessment or evaluation.

Whereas the HIPAA Privacy Rule requires an "authorization" for uses and disclosures of PHI not otherwise permitted or required, nearly all disclosures allowed under Part 2 require specific patient consent, and a patient consent form must contain certain elements to be valid, including the purpose of the disclosure, the name of the person/entity who is to receive the information, and a date or condition upon which the consent expires.[105] However, Part 2 does include certain narrow provisions and exceptions where disclosure is allowed without patient consent.[106] These include communications within a program or between a program and an entity having direct administrative control over that program (e.g., the staff of a detoxification unit within a hospital can share information with hospital administrators where needed to provide substance abuse services to the program's patients). In addition, communications are allowed without patient consent between a program and a qualified service organization (e.g., a person or entity that provides services such as data processing, bill collection, or accounting to a program) when the information exchanged is needed to provide the covered services.[107] Part 2 also allows disclosure without patient consent in strictly defined circumstances for medical emergencies,[108] audit or evaluation activities,[109] and scientific research purposes.[110]

The fact that patient-identifying information may be disclosed pursuant to one of the exceptions to Part 2's general rule does not mean that the disclosed information is no longer protected by the regulations. Part 2 generally prohibits anyone who receives information from a substance abuse program from re-disclosing it, and requires that any information released must be accompanied by a written notice informing the recipient that federal law prohibits its re-disclosure unless expressly permitted by the patient or as otherwise authorized by the regulations.[111]

B. Part 2 in the correctional context

In the criminal justice context, it is notable that the legislation authorizing Part 2 explicitly states that: "[e] xcept as authorized by a court order … no [substance abuse] record … may be used to initiate or substantiate any criminal charges against a patient or to conduct any investigation of a patient."[112] Part 2 implements this requirement procedurally by specifying that a court order authorizing the disclosure and use of patient records for the purpose of conducting a criminal investigation or prosecution of a patient may be issued only if the court finds that: (1) the crime involved is extremely serious; (2) there is a reasonable likelihood that the records will disclose information of substantial value in the investigation or prosecution; (3) other ways of obtaining the information are not available or would not be effective; and (4) the potential injury to the patient, the physician-patient relationship, and the ability of the program to provide services to other patients is outweighed by the public interest and the need for the disclosure. Further, the order must limit disclosure and use of the information to those parts of the patient's record that are essential to fulfill the objective of the order.[113] These requirements are supported by the text of the re-disclosure notice that must accompany any information released pursuant to the regulations, which states that "Federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patient."[114] In general, court orders under Part 2 may authorize a disclosure or use of patient information that otherwise would be prohibited by the regulation, but cannot compel disclosure; a subpoena or similar legal mandate would have to be issued simultaneously in order to compel disclosure.[115]

Although the HIPAA Privacy Rule contains disclosure provisions specific to correctional institutions/custodial situations and law enforcement, Part 2 does not. That is, other than in the case of medical emergencies, a patient's commission of a crime on the premises of

a program or against program personnel (or threat to commit such a crime),[116] or reports of suspected child abuse and neglect under state law,[117] law enforcement officers likely will require court orders for obtaining information from a Part 2 program. In addition, disclosure to or from a correctional facility will most likely require patient consent or a court order. In general, court orders authorizing disclosure for noncriminal purposes require good cause, based upon the court's findings that other ways of obtaining the information are not available or would not be effective and the public interest and need for the disclosure outweigh the potential injury to the patient, the physician-patient relationship and the treatment services.[118] Court orders authorizing the disclosure of confidential communications made by a patient to a program in the course of diagnosis, treatment, or referral for treatment may be made only if the disclosure is necessary to protect against an existing threat, to assist in the investigation of a serious crime, or in connection with litigation or an administrative proceeding in which the patient offers testimony or other evidence pertaining to the content of the confidential communications.[119]

Also in contrast to the HIPAA Privacy Rule, which expressly excepts inmates from the general right it grants to individuals to receive notice of the uses and disclosures of PHI that a covered entity may make and of the individual's rights and the covered entity's legal duties with respect to PHI, Part 2 requires that programs notify all patients—with no exception for inmates—that federal law and regulations protect the confidentiality of alcohol and drug abuse patient records and give them a written summary of the regulations' requirements.[120]

Finally, Part 2 makes explicit allowance for disclosures to persons within the criminal justice system that have made participation in a program a condition of the disposition of any criminal proceedings against a patient (e.g., as part of a drug court program or other treatment-based alternative to incarceration) or of the patient's parole or other release from custody. A program may disclose information about a patient in this case only to those individuals who have a need for the information in connection with their duty to monitor the patient's progress (such as probation or parole officers responsible for supervision of the patient) and may do so only if the patient has signed a written consent in compliance with the regulation. Further, the patient's consent must specify a reasonable amount of time during which it will remain in effect, taking into account the anticipated length of the treatment, the type of criminal proceeding involved, the need for the information in connection with the final disposition of that proceeding, and when the final disposition will occur. Whereas the general requirement for most Part 2 disclosures is that written consent must include a statement that the consent is subject to revocation at any time, this particular provision of Part 2 requires instead that the written consent must state that it is revocable upon the passage of a specified amount of time or the occurrence of a specified event (which may be no later than the final disposition of the conditional release or other action in connection with which consent was given). Anyone who receives patient information under this provision of Part 2 (such as a probation officer) may re-disclose and use it only to carry out that person's official duties with regard to the patient's conditional release or other action in connection with which the consent was given.[121]

Like HIPAA, Part 2 sets a federal privacy floor. State laws that are less protective regarding disclosure and use of information about individuals in federally assisted alcohol or drug abuse treatment programs are pre-empted, while state laws that are more stringent are preserved.[122]

After the passage of HIPAA and promulgation of the Privacy Rule, DHHS issued guidance for substance abuse treatment programs that are subject to Part 2 in an effort to ease the transition and compliance with both laws. According to the guidance, the Privacy Rule and Part 2 requirements parallel each other in many areas. In the rare cases of conflict, it is recommended that substance abuse treatment programs should generally continue to follow the Part 2 regulations, as those rules are considered more protective of privacy.[123] Overall, the vast majority of states essentially have adopted Part 2 as the standard for protecting this type of health information.[124]

The future of health information-sharing in the correctional environment

In the context of electronic health information exchange, stakeholders have expressed concern that privacy laws present challenges to the development of policies and practices for information-sharing, particularly in the area of patient consent. States in particular vary widely in their requirements for consent and disclosure related to PHI—they differ, for example, in the way their statutes address types of PHI, PHI holders, recipients of PHI, different treatment scenarios, consent processes and forms, and requirements for HIPAA's minimum necessary standard. In sum, this lack of uniformity is often viewed as one of the most daunting challenges of implementing electronic exchange.[125]

These concerns, of course, apply within the correctional context as well. In the special case of Part 2 (and state laws based upon Part 2), although the law allows patient information to be disclosed to health information organizations (HIOs) and other health information exchange systems,[126] some entities perceive the policies and technical requirements that would need to be developed to enable that exchange as prohibitively complicated. Because nearly all disclosures pursuant to Part 2 require a detailed written patient consent, an electronic exchange would be required to develop a means of ensuring and documenting the consent as well as the capability of managing the information in order to comply with the law. It is therefore possible that the operators of these entities could choose to exclude data covered by Part 2 or the provider institutions likely to contribute such data from some electronic exchange operations. These concerns, of course, are not unique to Part 2—similar issues are raised by state health information disclosure laws that require consent for the disclosure of other types of health information. In addition, HIOs might face these questions independent of any legal requirements depending on the policies they adopt for making clinical information available to participating members. That is, if an HIO chooses to require affirmative patient consent for participation, a covered entity or program covered by Part 2 would need to obtain patient consent to disclose information to the HIO even where it might not otherwise be legally required (e.g., where a business associate or qualified service organization agreement is already in place between the entities).[127]

It has been suggested that the segmentation or sequestering of specific (i.e., "sensitive") health information/data might offer a path forward that both enables electronic exchange of the information and ensures its protection and compliance with the law. The term "data segmentation" refers to "the process of sequestering from capture, access or view certain data elements that are perceived by a legal entity, institution, organization, or individual as being undesirable to share."[128] The process provides a potential means of protecting specific elements of health information, both within an EHR and in the broader electronic exchange context, which could prove useful in implementing current legal requirements and honoring patient choice. For example, where a substance abuse treatment program is part of a larger entity with multiple departments generating data for the same patient, data segmentation might enable the exchange of certain elements within that patient's record without violating Part 2's requirements for disclosure. Data segmentation could also be used to help patients express their preferences with regard to health information-sharing, thereby supporting underlying principles of personal autonomy as well as enhancing patient trust and encouraging patient engagement in their health care.[129] The Office of the National Coordinator (ONC) for Health Information Technology at DHHS, the principal federal entity charged with coordinating nationwide efforts to implement and use health IT and the electronic exchange of health information, is currently exploring the use of data segmentation for privacy purposes under the auspices of the ONC Standards & Interoperability Framework. The goal of the initiative is to produce a pilot project that allows providers to share portions of an EHR while not sharing others, such as information related to substance abuse treatment.[130]

One example of data segmentation in the behavioral health and substance abuse context is provided by the Texas Department of State Health Services Clinical Management for Behavioral Health Services (CMBHS), an EHR system developed to serve behavioral health

and substance abuse providers in the State of Texas. CMBHS uses data segmentation to enable health information-sharing based on a patient's consent preferences, although the system does not yet allow for interoperable electronic exchange of the data—that is, electronic exchange can occur only among providers using the same system. The system allows a patient to release an entire record or segment categories in order to exchange only specific data. Providers work with patients to complete an electronic consent form that indicates which types of clinical documents may be released, which providers may have access to those documents, a date range for access and an expiration date of the consent. Hard copies of the consent form are also signed by patients and saved in the system, at which point the indicated providers have access to the information until the expiration date of the consent. Once information is shared with one provider in the system, other providers within that provider's organization can access the information. The system automatically prompts a provider to request patient consent in the case of referrals to providers outside the organization.[131]

Other methods of facilitating electronic health information-sharing while appropriately protecting patient privacy have been explored. For example, DHHS has released guidance that indicates that Part 2 would allow the use of single consent forms for multiple disclosures as well as multiple-party consent forms. A single consent form could be used to authorize a disclosure of information about a patient to one recipient, such as an HIO, and simultaneously authorize that recipient to re-disclose the information to an additional entity or entities (such as other health care providers affiliated with the HIO and identified in the consent form), provided that the purpose for the disclosure is the same. In addition, if a patient wished to authorize all or many members of an HIO to access his/her Part 2-protected record as well as to exchange information with one another, a multiple-party consent form could be developed that includes a list of the names of each person or organization to whom disclosures may be made; states that the parties may disclose to each other; and gives the allowable purposes for those disclosures. In this case, the consent form must authorize each party to disclose to the other ones particular information for a particular purpose. In both scenarios, the required statement prohibiting re-disclosure would have to accompany the information disclosed, so that each subsequent recipient of the information is notified of the prohibitions on re-disclosure.[132]

Methods of facilitating health information-sharing have been explored within the correctional environment as well. Jurisdictions have developed a variety of approaches to sharing information based on individualized local circumstances, including state law, such as co-locating criminal justice and mental health practitioners, developing procedures to obtain permission forms or court orders, and contracting with business associates and qualified service organizations. In particular, jurisdictions have developed such information-sharing tools as uniform authorization/consent forms and standard judicial orders, which could ease the sharing of health information within and across systems. As obtaining permission from an individual to release his/her health information is the most straightforward way of facilitating information-sharing, authorization or consent forms can be obtained at various stages in the criminal justice process, such as booking in a jail or when joining a mental health court or other diversion program. Uniform consent forms that comply with both federal and state law requirements could be written to include all major entities in the collaborative system, allowing the individual to choose among them, provided that the special requirements for Part 2 consents, in particular, are followed closely.[133]

Finally, as described above, Part 2 permits disclosures to persons within the criminal justice system who have made participation in a substance abuse program a condition of the disposition of criminal proceedings against a patient or of the patient's parole or release from custody as long as the patient has signed a written consent in compliance with the regulation. This type of process has also proved useful in mental health courts, which require the collection and sharing of information about participants at all points of the court process, from the initial screening and eligibility determination throughout the entire period of judicial supervision. These courts have found that asking mental health court

participants upon entry into the system to provide their written consent to release information on a form that specifically identifies what information will be released and to whom helps facilitate information-sharing and compliance with legal requirements.[134]

Conclusion

Health information-sharing in correctional institutions occurs within the context of complex and evolving privacy law. The purpose of these state and federal laws is to protect patients' most personal information and thereby encourage their active participation in their own health care. While pursuit of these goals is sometimes adjusted in the correctional environment due to other legitimate societal interests, the underlying values and policy choices remain the same. Yet, the implications of and possibilities for health information-sharing in this context with appropriate privacy protections in place should not be overlooked. About 4% of jail admissions result in prison sentences; that is, 96% of jail detainees and inmates return directly to the community from jail, along with their often-untreated health conditions.[135] Many detainees are released on bail pending trial after just several hours or a few days, with 64% of the jail population turning over every week.[136] Moreover, half of the jail population is confined for a probation or parole violation or for bond forfeiture, which indicates at base the repeat nature of incarceration.[137]

Once they have returned to the community, inmates released from secure correctional facilities represent 17% of the total AIDS population, 13% to 19% of those with HIV, 12% to 16% of those with hepatitis B, 20% to 32% of those with hepatitis C and 35% of those with tuberculosis."[138] The ancillary effects of the health problems in this population on our society as a whole can be enormous, from the potential to spread communicable diseases to the effects of substance abuse and untreated psychiatric disorders. To date, expanding the use of health IT in the correctional environment has not been a major focus of state or federal policymakers, although the use of EHRs does seem to be slowly increasing. The potential of health IT for this population is clear, however: the chance to improve the quality, safety and efficiency of health care for a high-risk subset of Americans who have the likelihood of widely affecting the public's health. The widespread use of EHRs and, eventually, electronic exchange in the correctional environment could play an important role in helping stabilize the health care of inmates while in correctional institutions as well as help ease their re-entry into the community.

This paper was commissioned by COCHS, whose work is facilitated by Rosenberg and Associates through a contract with the Robert Wood Johnson Foundation.

Endnotes

1 Goldstein MM and Blumenthal D. "Building an Information Technology Infrastructure." *Journal of Law, Medicine and Ethics*, 36(4): 709-715, at 712, December 2008.

2 Goldstein MM and Rein AL. *Consumer Consent Options for Electronic Health Information Exchange: Policy Considerations and Analysis.* Washington: US Department of Health and Human Services, Office of the National Coordinator for Health Information Technology, March 2010, http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11673_911197_0_0_18/ChoiceModelFinal032610.pdf, (accessed March 2012).

3 *See Making it Meaningful: How Consumers Value and Trust Health IT*. Washington: National Partnership for Women and Families, February 2012, http://www.nationalpartnership.org/site/PageServer?pagename=issues_health_IT_survey (accessed March 2012).

4 *One in 100: Behind Bars in America 2008*. Washington: The Pew Charitable Trusts, 2008, http://www.pewcenteronthestates.org/report_detail.aspx?id=35904 (accessed March 2012).

5 Minton TD. *Jail Inmates at Midyear 2010 - Statistical Tables*. Washington: US Department of Justice, Bureau of Justice Statistics, NCJ 233431, April 2011, http://www.bjs.gov/index.cfm?ty=pbdetail&iid=2375 (accessed March 2012). Prisons are correctional institutions designated by federal or state law for the confinement of offenders who are judicially ordered into custody for punishment. Jails are locally operated correctional facilities that confine accused persons awaiting trial and incarcerate convicted individuals usually up to one year, usually for misdemeanor offenses. *See* Freudenberg N. "Jails, Prisons, and the Health of the Urban Populations: A Review of the Impact of the Correctional System on Community Health." *Journal of Urban Health*, 78:214-235, 2001.

6 Conklin TJ, Lincoln T and Wilson DR. *A Public Health Manual for Correctional Health Care*. Ludlow, MA: Hampden County Sheriff's Department, October 2002, http://www.mphaweb.org/documents/PHModelforCorrectionalHealth.pdf (accessed March 2012).

7 Binswanger IA, Krueger PM and Steiner JF. "Prevalence of Chronic Medical Conditions Among Jail and Prison Inmates in the USA Compared with the General Population." *Journal of Epidemiology and Community Health*, 63(11): 912-919, November 2009.

8 Steadman HJ, Osher FC, Robbins PC, et al. "Prevalence of Serious Mental Illness Among Jail Inmates." *Psychiatric Services*, 60(6): 761–765, June 2006.

9 Karberg JC and James DJ. *Substance Dependence, Abuse, and Treatment of Jail Inmates, 2002*. Washington: US Department of Justice, Bureau of Justice Statistics, NCJ 209588, July 2005, http://www.bjs.gov/index.cfm?ty=pbdetail&iid=1128 (accessed March 2012).

10 Conklin TJ, Lincoln T and Wilson DR, *A Public Health Manual*.

11 Damberg CL, Shaw R, Teleki SS, et al. "A review of Quality Measures Used by State and Federal Prisons." *Journal of Correctional Health Care*, 17(2): 122-137.

12 "Texas Curbs Spending by $1B by Deploying EHRs, Telehealth in Prisons," *iHealthBeat*, August 26, 2011, http://www.ihealthbeat.org/articles/2011/8/26/texas-curbs-spending-by-1b-by-deploying-ehrs-telehealth-in-prisons.aspx (accessed March 2012); *see also* "Telemedicine and EHR Use for Inmates Helps Save State $1B," *FierceEMR*, August 25, 2011, http://www.fierceemr.com/story/ehr-use-inmates-helps-save-state-1b/2011-08-25 (accessed March 2012).

13 Woodard A. "Data Tech Can Lower Prison Expense," *Atlanta Journal-Constitution*, August 2, 2011, http://www.ajc.com/opinion/data-tech-can-lower-1069305.html (accessed March 2012).

14 "City of Philadelphia Selects eClinicalWorks for Electronic Health Records," *FierceEMR*, May 16, 2011, http://www.fiercehealthcare.com/press-releases/city-philadelphia-selects-eclinicalworks-electronic-health-records (accessed March 2012).

15 Wingett Y and Hensley JJ, "In Wake of Suits, Maricopa County Tackles Jail-Inmate Care," *AZCentral.Com*, May 11, 2010, http://www.azcentral.com/community/phoenix/articles/2010/05/11/20100511maricopa-county-jail-inmate-care.html (accessed March 2012).

16 "Los Angeles County approves $17M for EMR in juvenile detention facilities," *FierceEMR*, June 3, 2010, http://www.fierceemr.com/story/l-county-approves-17m-emr-juvenile-detention-facilities/2010-06-03 (accessed March 2012).

17 Goldstein MM. "Health Information Technology and the Idea of Informed Consent." *Journal of Law, Medicine, and Ethics*, 38(1): 27-35, March 2010. A detailed discussion of the ethical and legal issues surrounding an inmate's right to informed consent for treatment purposes is beyond the scope of this article.

18 Terry NP and Francis LP. "Ensuring the Privacy and Confidentiality of Electronic Health Records." *University of Illinois Law Review*, 2007(2): 681-736, February 2007.

19 Goldstein MM, *Idea of Informed Consent*, 27-35.

20 *Standards for Health Services in Jails*. Chicago: National Commission on Correctional Health Care, at 15-16, 2008.

21 Ibid, 116.

22 APHA Task Force on Correctional Health Care Standards. *Standards for Health Services in Correctional Institutions*, 7. Washington: American Public Health Association, 2003.

23 Pinta, ER. "Decisions to Breach Confidentiality When Prisoners Report Violations of Institutional Rules." *Journal of The American Academy of Psychiatry and the Law*, 37(2): 150-154, June 2009; *see also* APHA Task Force on Correctional Health Care Standards, *Standards for Health Services*, 7.

24 Seal DW, Eldridge GD, Zack B, et al. "HIV Testing and Treatment with Correctional Populations: People, Not Prisoners." *Journal of Health Care for the Poor and Underserved*, 21(3): 977-985, at 980, August 2010.

25 District of Columbia Department of Corrections. *DC Department of Corrections Facts and Figures*. October 2011, http://doc.dc.gov/doc/frames.asp?doc=/doc/lib/doc/populationstats/DCDepartmentofCorrectionsFactsnFiguresOct11corrected.pdf (accessed March 2012).

26 *See* Tauber J, Weinstein SP and Taube D. *Federal Confidentiality Laws and How They Affect Drug Court Practitioners*. Alexandria, VA: National Drug Court Institute, April 1999, https://www.ncjrs.gov/App/publications/Abstract.aspx?id=179655 (accessed March 2012).

27 *See* Goldstein MM, Repasch L and Rosenbaum S. "Emerging Privacy Issues in Health Information Technology," in *Health Information Technology in the United States: Where We Stand, 2008*, Blumenthal D et al. (eds), 92-103, at 96 (citing *Whalen v. Roe*, 429 U.S. 589 (1977)). Washington: Robert Wood Johnson Foundation, 2008, http://www.rwjf.org/pr/product.jsp?id=31831 (accessed March 2012).

28 *See* Cohen F. "No Medical Records Privacy for Inmate in Sexual Predator Commitment Proceeding." *Correctional Law Reporter*. Civic Research Institute, at 35, October/November 2010 (citing *Seaton v.* Mayberg, 610 F.3d 530 (9th Cir. 2010); *Doe v. Delie*, 257 F.3d 309, 311 (3d Cir. 2011); and *Powell v. Schriver*, 175 F.3d 107, 112 (2d Cir. 1999)).

29 National Commission on Correctional Health Care, *Standards for Health Services*, 138 (citing *Woods v. White*, 689 F. Supp. 874 (W.D. Wis. 1988) and *Powell v. Schriver*, 175 F.3d 107, 112 (2d Cir. 1999), respectively).

30 Gostin LO et al. "The Law and the Public's Health: A Study of Infectious Disease Law in the United States." *Columbia Law Review*, 99(1): 59-128, January 1999.

31 Goldstein MM and Rein AL, *Consumer Consent Options*.

32 Pritts JD. "The Importance and Value of Protecting the Privacy of Health Information: The Roles of the HIPAA Privacy Rule and the Common Rule in Health Research." Washington: National Academy of Sciences, at 12, 2008, http://www.iom.edu/~/media/Files/Activity%20Files/Research/HIPAAandResearch/PrittsPrivacyFinalDraftweb.ashx (accessed March 2012).

33 45 C.F.R. §§ 160, 164.

34 45 C.F.R. § 160.203.

35 Goldstein MM, Repasch L and Rosenbaum S, "Emerging Privacy Issues."

36 Consumer Partnership for eHealth. *Protecting Sensitive Health Information*, 2-3, June 2010, http://www.nationalpartnership.org/site/DocServer/Sensitive-Data-Final_070710__2_.pdf?docID=7041.

37 *See* Petrila J. *Dispelling the Myths about Information Sharing Between the Mental Health and Criminal Justice Systems*. The CMHS National GAINS Center for Systemic Change for Justice-Involved People With Mental Illness, at 3, February 2007, http://gains.prainc.com/pdfs/integrating/Dispelling_Myths.pdf (accessed March 2012); 45 C.F.R. § 164.512(3).

38 45 C.F.R. § 160.103.

39 Ibid.

40 45 C.F.R. § 164.502(a).

41 45 C.F.R. § 164.502(a)(2).

42 A list of permitted disclosures may be found at 45 C.F.R. § 164.502(a)(1).

43 45 C.F.R. § 164.520.

44 45 C.F.R. § 164.502(b).

45 Ibid.

46 45 C.F.R. § 164.508(a).

47 45 C.F.R. § 164.508(c)(1).

48 45 C.F.R. § 164.506(a).

49 US Department of Health and Human Services, Office for Civil Rights. *Summary of Privacy Rule*, 5, 2003, http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf (accessed March 2012).

50 45 C.F.R. § 164.512(e).

51 45 C.F.R. § 164.512(f).

52 45 C.F.R. § 164.512(j).

53 45 C.F.R. § 164.512(k)(5).

54 US Department of Health and Human Services, Office for Civil Rights. *What Is the Difference Between "Consent" and "Authorization" Under the HIPAA Privacy Rule?* 2003, http://www.hhs.gov/ocr/privacy/hipaa/faq/use/264.html (accessed March 2012).

55 45 C.F.R. § 164.508(b)(4).

56 Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII, Division A of the American Recovery and Reinvestment Act (ARRA), Pub. L. No. 111-5, §§ 13001-13424, 123 Stat. 115, 228-279 (2009); *see generally* Goldstein MM, Repasch L and Rosenbaum S. "Recent Federal Initiatives in Health Information Technology," in *Health Information Technology in the United States, 2009: On the Cusp of Change*," DesRoches CM and Jha AK (eds), 60-69. Washington: Robert Wood Johnson Foundation, 2009, http://www.rwjf.org/pr/product.jsp?id=50308 (accessed March 2012).

57 McGraw D. "Privacy and Health Information Technology." *O'Neill Institute: Legal Solutions in Health Reform*, 7, April 2009, http://www.law.georgetown.edu/oneillinstitute/national-health-law/legal-solutions-in-health-reform/Privacy.html (accessed March 2012).

58 HITECH § 13408, 123 Stat. 115, 271 (2009). Pursuant to HIPAA, "business associates" are entities that perform activities on behalf of, or provide certain services to, covered entities that involve the use or disclosure of individually identifiable health information. 45 C.F.R § 160.103 (2009).

59 HITECH §§ 13401, 13404, 123 Stat at 260, 264 (2009).

60 Ibid.

61 *See generally* HITECH §§ 13409, 13410 (2009).

62 Department of Health and Human Services, Standards for Privacy of Individually Identifiable Health Information; Proposed Rule, 64 Fed. Reg. 59918-60065, 59938 (November 3, 1999).

63 Department of Health and Human Services, Standards for Privacy of Individually Identifiable Health Information; Final Rule, Preamble, 65 Fed. Reg. 82462-82829, at 82540-82541, 82622 (Dec. 28, 2000).

64 *See* US Department of Health and Human Services, Centers for Medicare and Medicaid Services (CMS). *Covered Entity Charts: Guidance on How to Determine Whether an Organization or Individual is a Covered Entity Under the Administrative Simplification Provisions of HIPAA*, http://www.cms.gov/HIPAAGenInfo/Downloads/CoveredEntitycharts.pdf (accessed March 2012).

65 "Health care provider" is defined as "a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business." 45 C.F.R. § 160.103.

66 45 C.F.R. §§ 162 Subparts J-R; *See* CMS, *Covered Entity Charts*.

67 *See, e.g.,* Bizzell WD. "The Protection of Inmates' Medical Records: The Challenge of HIPAA Privacy Regulations," *corrections.com*, February 24, 2003, http://www.corrections.com/articles/11103-the-protection-of-inmates-medical-records-the-challenge-of-hipaa-privacy-regulations (accessed March 2012); CMS, *Covered Entity Charts*, 7 ("If a healthcare provider uses another entity (such as a clearinghouse) to conduct covered transactions in electronic form on its behalf, the health care provider is considered to be conducting the transaction in electronic form.").

68 Bizzell WD, "The Protection of Inmates' Medical Records."

69 *See, e.g.*, Orr D and Hellerstein D. "Controversy, Confusion Herald HIPAA." *CorrectCare, National Commission on Correctional Health Care*, 2002, http://www.ncchc.org/pubs/CC/hipaastudy.html (accessed March 2012); Shimkus J, "HIPAA Is Here. What Does It Mean For You?" *CorrectCare, National Commission on Correctional Health Care*, 2003, http://www.ncchc.org/pubs/CC/hipaaishere.html (accessed March 2012).

70 Shimkus J, "Controversy, Confusion."

71 Petrila J and Fader-Towe H. "Information Sharing in Criminal Justice-Mental Health Collaborations: Working with HIPAA and Other Privacy Laws." *Council of State Governments Justice Center*, 2010, http://consensusproject.org/jc_publications/info-sharing (accessed March 2012).

72 Department of Health and Human Services, Final Rule, Preamble, 65 Fed. Reg. at 82622.

73 Ibid.

74 *Correctional institution* is defined by the Rule as "any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. *Other persons* held in lawful custody includes juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial." 45 C.F.R. § 164.501. *Inmate* is defined as "a person incarcerated in or otherwise confined to a correctional institution." Ibid.

75 *See* Bizzell WD, "The Protection of Inmates' Medical Records."

76 45 C.F.R. § 164.512(k)(5).

77 Department of Health and Human Services, Final Rule, Preamble, 65 Fed. Reg. at 82541, 82622.

78 45 C.F.R. § 164.512(b).

79 45 C.F.R. § 164.512(e).

80 45 C.F.R. § 164.512(f).

81 45 C.F.R. § 164.512(j).

82 45 C.F.R. § 164.512(c).

83 45 C.F.R. § 164.512(a).

84 45 C.F.R. § 164.512(f). Covered entities are also allowed to disclose PHI to law enforcement officials as required by law pursuant to a court order, warrant, subpoena, or administrative request; in response to a law enforcement official's request for information about an individual who is or is suspected to be a victim of a crime; to alert law enforcement of the death of an individual if the covered entity suspects that death may have resulted from criminal conduct; when the covered entity believes in good faith that the PHI constitutes evidence of criminal conduct that occurred on the premises of the covered entity; and, in the case of a medical emergency not on the premises of the covered entity if the disclosure appears necessary to alert law enforcement to the commission, nature, or location of a crime, crime victim, or perpetrator. Ibid.

85 45 C.F.R. § 164.512(j).

86 45 C.F.R. § 164.512(e).

87 45 C.F.R. § 164.520(a).

88 Department of Health and Human Services, Final Rule, Preamble, 65 Fed. Reg. at 82548.

89 National Commission on Correctional Health Care, *Standards for Health Services*, 116.

90 45 C.F.R. § 164.524(a).

91 Department of Health and Human Services, Final Rule, Preamble, 65 Fed. Reg. at 82555.

92 45 C.F.R. § 164.526.

93 *See generally* Goldstein MM and Rein AL, *Consumer Consent Options*, 45-47.

94 The Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment and Rehabilitation Act of 1970, Pub. L. No. 91-616, 84 Stat. 1848, and the Drug Abuse Office and Treatment Act of 1972, Pub L. No. 92-255, 86 Stat. 65. The rulemaking authority granted by both statutes relating to confidentiality of records can now be found at 42 U.S.C. § 290dd-2 (2006) and the regulations themselves at 42 C.F.R. Part 2.

95 H. Rep. No. 92-775, at 24 (1972), *reprinted in* 1972 U.S.C.C.A.N. 2045, 2072.

96 Westley HC. "Federal Substance Use Disorder Confidentiality." *US Department of Health and Human Services, Substance Abuse and Mental Health Services Administration*, 31, 50, April 2010, http://www.ncsapa.org/download/34/ (accessed March 2012).

97 42 C.F.R. § 2.3(a).

98 42 C.F.R. §§ 2.11, 2.13(a).

99 *See* Lopez F. "Confidentiality of Patient Records for Alcohol and Other Drug Treatment," in *Technical Assistance Publication (TAP) Series 13*. Washington: US Department of Health and Human Services, Substance Abuse and Mental Health Services Administration, 1994, http://kap.samhsa.gov/products/manuals/taps/13b.htm (accessed March 2012).

100 42 C.F.R. § 2.11.

101 A program is "federally assisted" if it is 1) authorized, licensed, certified, or registered by the federal government; 2) receives federal funds in any form, even if the funds do not directly pay for the alcohol or drug abuse services; or 3) is assisted by the Internal Revenue Service through a grant of tax exempt status or allowance of tax deductions for contributions; or 4) is authorized to conduct business by the federal government (e.g., certified as a Medicare provider, authorized to conduct methadone maintenance treatment, or registered with the Drug Enforcement Agency (DEA) to dispense a controlled substance used in the treatment of alcohol or drug abuse); or 5) is conducted directly by the federal government. In practice, most drug and alcohol treatment programs are federally assisted. 42 C.F.R. § 2.12; *see also* Legal Action Center, "Frequently Asked Questions: Applying the Substance Abuse Confidentiality Regulations to Health Information Exchange (HIE)," *US Department of Health and Human Services, Substance Abuse and Mental Health Services Administration*, at 2-3, June 2010, http://www.samhsa.gov/healthprivacy/docs/EHR-FAQs.pdf (accessed March 2012).

102 42 C.F.R. § 2.11.

103 42 C.F.R. §§ 2.11, 2.12(e)(1).

104 42 C.F.R. § 2.11.

105 Written consent forms under Part 2 must include: (1) The specific name or general designation of the program or person permitted to make the disclosure; (2) The name or title of the individual or the name of the organization to which disclosure is to be made; (3) The name of the patient; (4) The purpose of the disclosure; (5) How much and what kind of information is to be disclosed; (6) The signature of the patient and, when required for a patient who is a minor, the signature of a person authorized to give consent; or, when required for a patient who is incompetent or deceased, the signature of a person authorized to sign in lieu of the patient; (7) The date on which the consent is signed; (8) A statement that the consent is subject to revocation at any time except to the extent that the program or person which is to make the disclosure has already acted in reliance on it. Acting in reliance includes the provision of treatment services in reliance on a valid consent to disclose information to a third party payer; and (9) The date, event, or condition upon which the consent will expire if not revoked before. This date, event, or condition must insure that the consent will last no longer than reasonably necessary to serve the purpose for which it is given. 42 C.F.R. § 2.31.

106 42 C.F.R. § 2.12.

107 42 C.F.R. §§ 2.11, 2.12. Qualified service organizations must sign agreements acknowledging that they are fully bound by the regulations, and that, if necessary, they will resist in judicial proceedings any efforts to obtain access to patient records except as permitted by the regulations. Ibid.

108 42 C.F.R. § 2.51.

109 42 C.F.R. § 2.53.

110 42 C.F.R. § 2.52.

111 42 C.F.R. § 2.32.

112 42 U.S.C. § 290dd-2(c) (2006).

113 42 C.F.R. § 2.65(d) and (e); *see also* Snavely KR, Taxman FS and Gordon S. "Offender-Based Information Sharing: Using a Consent-Driven System to Promote Integrated Service Delivery," in *Information Technology and the Criminal Justice System*, Pattavina A (ed), at 195-219. Thousand Oaks, CA: Sage Publications, Inc., 2005.

114 42 C.F.R. § 2.32.

115 42 C.F.R. § 2.61.

116 42 C.F.R. § 2.12. Disclosures related to crimes on program premises or against program personnel must be limited to the circumstances of the incident and the patient's status, name, address, and last known whereabouts.

117 42 C.F.R. § 2.12.

118 42 C.F.R. § 2.64.

119 42 C.F.R. § 2.63. *See also* Petrila J and Fader-Towe H, "Information Sharing in Criminal Justice-Mental Health Collaborations," 5.

120 42 C.F.R. § 2.22.

121 42 C.F.R. § 2.35.

122 42 C.F.R. § 2.20.

123 *See* "The Confidentiality of Alcohol and Drug Abuse Patient Records Regulation and the HIPAA Privacy Rule: Implications for Alcohol and Substance Abuse Programs." *US Department of Health and Human Services, Substance Abuse and Mental Health Services Administration*, June 2004, http://www.SAMHSA.GOV/HealthPrivacy/docs/SAMHSAPart2-HIPAAComparison2004.pdf (accessed March 2012).

124 Pritts J, Lewis S, Jacobson R, et al. *Privacy and Security Solutions for Interoperable Health Information Exchange: Report on State Law Requirements for Patient Permission to Disclose Health Information*. Chicago: RTI International, 3-1, 3-13, August 2009, http://www.healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10741_910326_0_0_18/DisclosureReport.pdf (accessed March 2012).

125 Goldstein MM and Rein AL, *Consumer Consent Options*, 48.

126 In general, a Part 2 program would need to ensure that either a patient consent or a qualified service organization agreement is in place in order for the program to disclose the information to an HIO. In addition, patient consent would be needed for the HIO to redisclose the information to other specified HIO affiliated members and any disclosures must be accompanied by an accompanying notice explaining the general prohibition on redisclosure. *See* Legal Action Center, "Frequently Asked Questions."

127 *See* Goldstein MM and Rein AL, *Consumer Consent Options*, 46-47.

128 Goldstein MM and Rein AL. *Data Segmentation in Electronic Health Information Exchange: Policy Considerations and Analysis*. Washington: US Department of Health and Human Services, Office of the National Coordinator for Health Information Technology, 2, September 2010, http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11673_950145_0_0_18/gwu-data-segmentation-final.pdf (accessed March 2012).

129 Ibid.

130 *See* "Data Segmentation for Privacy Homepage," S&I Framework, http://wiki.siframework.org/Data+Segmentation+for+Privacy+Homepage (accessed March 2012).

131 Goldstein MM and Rein AL, *Data Segmentation*, 45-46. *See also* Texas Department of State Health Services. *BHIPS Functionality Definition*, March 2010, http://www.dshs.state.tx.us/sa/BHIPS/functionality.shtm (accessed March 2012).

132 Legal Action Center, "Frequently Asked Questions," 9-10.

133 *See* Petrila J and Fader-Towe H, "Information Sharing in Criminal Justice-Mental Health Collaborations," 3.

134 "A Guide to Mental Health Court Design and Implementation." *Council of State Governments Justice Center*, 31, 2005, http://consensusproject.org/jc_publications/guide-to-mental-health-court-implementation (accessed March 2012).

135 Veysey B. *The Intersection of Public Health and Public Safety in U.S. Jails: Implications and Opportunities of Federal Health Care Reform*. Oakland, CA: Community Oriented Correctional Health Services, 2011, http://www.cochs.org/health_reform/PPACA_conference (accessed March 2012).

136 Minton TD. *Jail Inmates at Midyear 2009 - Statistical Tables*. Washington: US Department of Justice, Bureau of Justice Statistics, NCJ 230122, June 2010, http://www.bjs.gov/index.cfm?ty=pbdetail&iid=2195 (accessed March 2012).

137 Veysey B, *The Intersection of Public Health*.

138 Conklin TJ, Lincoln T and Wilson DR, *A Public Health Manual*; Veysey, B, *The Intersection of Public Health.*