Health Information Privacy and Health Information Technology in the US Correctional Setting

Melissa M. Goldstein, JD

Electronic health records and electronic health information exchange are essential to improving quality of care, reducing medical errors and health disparities, and advancing the delivery of patient-centered medical care. In the US correctional setting, these goals are critical because of the high numbers of Americans affected, yet the use of health information technology is quite limited.

In this article, I describe the legal environment surrounding health information sharing in corrections by focusing on 2 key federal privacy laws: the Health Insurance Portability and Accountability Act of 1996 and the federal Confidentiality of Alcohol and Drug Abuse Patient Records laws.

In addition, I review stakeholder concerns and describe possible ways forward that enable electronic exchange while ensuring protection of inmate information and legal compliance. (*Am J Public Health.* 2014;104:803–809. doi:10.2105/AJPH.2013.301845)

THE WIDESPREAD USE OF electronic health records (EHRs) and electronic health information exchange is essential to improving quality of care, reducing medical errors, decreasing health disparities, and advancing the delivery of patient-centered medical care.[1] At the same time, it is recognized that appropriate privacy and security policies must be established and enforced if we are to truly achieve the benefits of electronic exchange.[2]

In the US correctional setting, these goals are critical because of the number of Americans affected: in 2008, more than 2.3 million people were inmates on any given day, more than 1 in 100 American adults. Local jails admitted an estimated 11.6 million people during the 12 months ending June 30, 2012, with a midyear inmate population of 744 524.[4,5] (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 individuals awaiting trial and incarcerate convicted individuals, usually for up to 1 year and typically for misdemeanor offenses.[5])

The implications of and possibilities for health information sharing in this context through the use of health information technology with appropriate privacy protections in place should not be overlooked. Inmates at correctional facilities are a discrete population living in close contact, and maintaining accurate and easily accessible records is important to the overall health of the population. This population is also aging[6,7] and disproportionately ill, with high rates of health problems (e.g., chronic[8,9] and infectious disease,[10] injuries[11]), psychiatric disorders,[12,13] and substance use disorders.[14,15]

Furthermore, the jail population is transient: only about 4% of jail admissions result in prison sentences; 96% of jail detainees and inmates return directly to the community, along with their often-untreated health conditions.[16] Many detainees are released on bail pending trial after just several hours or a few days, with 60.2% of the jail population turning over every week.[4] Half of the jail population is confined as a result of probation or parole violations or bond forfeiture.[16]

Once 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.[15,16] The ancillary impact of the health problems in this population on society as a whole can be enormous, from the potential spread of communicable diseases to the effects of substance abuse and untreated psychiatric disorders.

The use of health information technology in correctional settings is quite limited, however. One recent study showed a range of technological sophistication among prison facilities, with rare use of EHRs.[17] Furthermore, there is very little electronic exchange of health information within correctional systems or between systems and community providers. There are signs that EHR use is increasing, however, including reported adoption by the Federal Bureau of Prisons,[18] the Texas Department of Criminal Justice,[19,20] and the Georgia Department of Corrections,[21] among others.[22–24] There also appears to be growing interest among government leaders at all levels in the potential of health information technology to help bridge the divide between jails and their communities.[25,26]

Here I explore the legal environment in which health information sharing occurs in correctional settings. Numerous state and federal laws shape this environment, but a comprehensive legal review is beyond the scope of this article. After a brief review of underlying principles, I focus on 2 key federal privacy laws: the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the federal Confidentiality of Alcohol and Drug Abuse Patient Records laws (hereafter Part 2).

The overarching purpose of these laws—encouraging and enhancing patient participation in the health care system—is sometimes modified in the correctional environment because of the drafters' recognition of public safety needs. Their application also varies depending on factual circumstances; that is, an institution's methods of health care delivery and its organizational/administrative structure might affect the determination of any particular legal question. In addition to reviewing stakeholder concerns regarding privacy law and the use of health information technology in the correctional environment, I describe possible ways forward that enable electronic exchange while ensuring protection of information and compliance with the law.

HEALTH INFORMATION PRIVACY LAW

Privacy and confidentiality laws support the expression of patient preferences and personal autonomy and encourage patient engagement.[27] Correctional health care standards reinforce these principles. According to the National Commission on Correctional Health Care, discussions 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" to protect patients' dignity and "foster necessary and candid conversation between patient and health care professional."[28(pp15–16)] The commission refers to the ethical obligations of health care practitioners as well:

> 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.[28(p116)]

Likewise, the American Public Health Association states that "[p]risoner-patients should be provided the same privacy of health care information as patients in the community,"[29] and American Bar Association standards mirror this perspective.[30] In the psychiatric context, inmates' concerns about confidentiality and lack of trust in staff have been identified as factors that prevent them from seeking mental health care.[29,31]

Although the US Constitution does not expressly provide a right to health information privacy, the US Supreme Court has recognized a limited right regarding information held in government databases. Attempts to assert that right more broadly have met with mixed results, leaving the question of constitutional protection of health information privacy unresolved.[32] In the correctional context, the few federal courts that have recognized a right to privacy in inmate medical records have held that it must give way when the state has a legitimate penological interest in accessing those records, such as the reporting of medical findings to prison and jail executives with a reason to know.[33]

Federal and state privacy laws have long been used to address the stigma and social hostility associated with particular health issues,[34] generally by limiting the exchange of certain health information without patient consent. Most states, for example, have laws protecting information in health records related to HIV, mental health conditions, and substance use.[35] The underlying purpose of such laws is generally to encourage greater participation and trust in the health care system through protection of a patient's private health information.[36] This patchwork of laws regarding "sensitive" information, however, is inconsistent and incomplete, making interpretation challenging, particularly for those initiating electronic exchange.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

The initial proposed version of the HIPAA Privacy Rule excluded inmates' health information from the definition of "protected health information" (PHI)[37] (individually identifiable health information held or transmitted in any form or medium by a covered entity or its "business associate," with limited exceptions), and therefore from HIPAA's protection, because "unimpeded sharing of inmate identifiable health information is crucial for correctional and detention facility operations."[38(p59938)] In response, the US Department of Health and Human Services received public comments to the proposed regulation arguing that the exclusion sent the message that abuses do not matter for this population. Commenters argued that inmates do 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. Upon release, disclosures could impair individuals' reintegration into society and subject them to discrimination. The drafters of the final regulation promulgated pursuant to the statute were persuaded and eliminated the exception.[39(pp82540–82541,82622)]

Central Elements of the Privacy Rule

HIPAA and the final Privacy Rule[40,41] provide a floor of privacy protection for health information; state laws that offer more stringent protections remain in force.[42] The rule governs the use and disclosure of PHI by "covered entities," that is, health plans, health care clearinghouses, and health care providers that transmit health information in electronic form in connection with certain transactions.[37]

Covered entities may not use or disclose PHI without patient authorization unless it is permitted or required by the Privacy Rule.[43] The rule requires disclosures of a patient's own PHI to the patient (although there is an exception to this requirement in the case of inmates, as described subsequently) and for enforcement purposes.[44] All other disclosures allowed without patient authorization are considered "permitted" under certain circumstances.[45] Uses and disclosures that are not

permitted or required by the rule require detailed written "authorizations"[46] from patients.

For example, the Privacy Rule permits covered entities to use and disclose PHI without written patient authorization for treatment, payment, and health care operations[47]; for judicial and administrative proceedings[48] and certain law enforcement purposes[49]; for the purpose of averting a serious threat to health or safety[50]; and for correctional institutions and other law enforcement custodial situations (as discussed subsequently).[51] The rule permits such uses or disclosures within certain parameters but does not require them; that is, covered entities are always free to seek authorization or to choose not to use or disclose the information.

HIPAA in the Correctional Context

Status as a covered entity. Within a jail system, inmates' health information may originate from or reside in many locations, including booking notes (e.g., infectious or chronic disease status), sick-call triage systems, physician notes, and other departments such as housing and work details (e.g., mobility or injury status). Such information might reside in the system regardless of an institution's status as a covered entity and therefore might not be protected by HIPAA.

The determination of whether any particular correctional institution is a covered entity can be difficult and requires careful analysis of the institution's operations. In general, an institution's status will likely depend on whether it qualifies as a health care provider (i.e., if it "furnishes, bills, or is paid for health care in the normal course of business"[37]) that transmits health information in electronic form in connection with certain transactions specified by the Privacy Rule.[52,53] Although correctional institutions are not likely to engage in most of the relevant transactions, it is conceivable that one might transmit clinical encounter information for the purpose of reporting health care, request a review of care to receive an authorization, or receive payment of claims from a private or public plan. If the institution or its health care component (e.g., prison clinic) electronically transmits these transactions or contracts with an entity that does so, it could be required to comply with HIPAA.[53,54]

For example, some analysts have concluded that county departments of corrections and local jails are required to comply with HIPAA if they bill electronically for inmate health care. That is, 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 could be considered a covered entity.[54] Because covered entity status hinges on electronic transmission of information, it is likely that the number of correctional institutions that qualify as covered entities will increase as the use of health information technology and electronic exchange within correctional systems increases.

Permitted uses and disclosures. Although the Privacy Rule does protect the health information of inmates, the drafters also recognized that correctional facilities have legitimate needs to use and share inmates' PHI without authorization.[39(p82622)] The rule therefore includes provisions regarding permissible uses and disclosures of inmates' PHI in the correctional context.

Covered entities may disclose the PHI of inmates without their authorization to correctional institutions[55] or law enforcement officials who have lawful custody of an inmate for the purpose of providing health care to the inmate or for the health and safety of the inmate, other inmates, the officers and employees of the institution and others at the facility, and those responsible for inmate transfer. Covered entities may also disclose the PHI of inmates without authorization for law enforcement purposes on the premises of an institution and for the administration and maintenance of the safety, security, and good order of the institution.[51]

These provisions apply only to the release of the PHI of current inmates.[51] When inmates are released, they have the same privacy rights under HIPAA as all other individuals.[39(pp82541,82622)]

Additional HIPAA provisions specific to inmates. The Privacy Rule also includes provisions regarding inmates' ability to exercise protections otherwise granted in the rule. Inmates are excluded from the right to receive notice of possible uses and disclosures of PHI and of their rights and a covered entity's duties with respect to PHI. Moreover, HIPAA's notice requirement does not apply at all to correctional institutions that qualify as covered entities.[56] Inmates have no right to notice regarding PHI created during incarceration, and correctional institutions are not required to send notices to inmates after release.

The Privacy Rule also excludes inmates from the right to obtain a copy of their PHI. Correctional institutions and health care providers acting under their direction may deny an inmate's request for a copy of his or her PHI if it would jeopardize the health, safety, security, custody, or rehabilitation of the inmate or other inmates or the safety of any officer, employee, or other person at the institution or responsible for transporting the inmate.[57] However, an inmate's request to inspect PHI must be granted unless one of the rule's other grounds for denial applies.[39(p82555)]

CONFIDENTIALITY OF ALCOHOL AND DRUG ABUSE RECORDS

Congress passed legislation in the early 1970s to encourage individuals to seek treatment for substance abuse and ensure that related information would be kept private. Those statutes and the accompanying regulations 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[58,59] (the rulemaking authority granted by these statutes relating to confidentiality of records can be found at 42 USC 290dd-2 and the regulations themselves at 42 CFR Part 2).

Central Elements of Part 2

The Part 2 regulations apply to information in any form that could reasonably be used to identify an individual and apply both to freestanding programs and programs that are part of larger organizations, such as substance abuse clinics in county jails.[60,61] Most disclosures under Part 2 require written patient consent that contains the purpose, the recipient's name, and an expiration date or condition for expiration.[62] However, Part 2 includes narrow exceptions wherein disclosure is allowed without consent,[63] including medical emergencies,[64] audit and evaluation activities,[65] and scientific research.[66] The regulations also require that information released from a substance abuse program be accompanied by a written notice stating that federal law prohibits its redisclosure unless expressly permitted by the patient or as otherwise authorized.[67]

As does HIPAA, Part 2 sets a federal privacy floor that allows more protective state laws.[68] Most states have adopted Part 2 as the standard for protecting such information.[69]

Part 2 in the Correctional Context

Part 2 does not contain disclosure provisions specific to correctional institutions, custodial situations, or law enforcement, so law enforcement officers and correctional institutions likely would require patient consent or court orders to obtain information from a Part 2 program unless an exception applies. Disclosure from a correctional facility covered by Part 2 most likely requires patient consent or a court order as well.

Court orders authorizing disclosure for noncriminal purposes require good cause, based on findings that other ways of obtaining the information are unavailable or ineffective and that the public need for disclosure outweighs potential injury to the patient, the physician–patient relationship, and the treatment services.[70] Although the requirements for court orders authorizing disclosure for conducting a criminal investigation or prosecution of a patient are similar, they also require that the crime involved be extremely serious and that there is a reasonable likelihood that the records will disclose information of substantial value. Such orders must limit disclosure and use of the information to those parts of patients' records that are essential to fulfill the orders' objectives.[71–73]

Finally, Part 2 allows disclosures to individuals within the criminal justice system who have made participation in a program a condition of the disposition of criminal proceedings against a patient (e.g., a drug court program) or of the patient's parole or release. Programs may disclose information only to those who need the information to monitor the patient's progress (e.g., probation or parole officers) and only with written patient consent. Anyone who receives patient information under this provision may use or redisclose it only to carry out official duties.[74]

FUTURE OF HEALTH INFORMATION SHARING AND PRIVACY

Stakeholders have expressed concern that privacy laws present challenges to the development of policies and practices for electronic information sharing, particularly in the area of patient consent. States, in particular, vary widely in the way statutes address types of PHI, holders and recipients of PHI, different treatment scenarios, and consent processes and forms. This lack of uniformity is often viewed as one of the most daunting challenges in implementing electronic exchange.[2]

These concerns also apply in the correctional context, wherein the structural tensions between increased use of technology and privacy produce similar challenges but the individuals involved (inmates) are sometimes afforded fewer privacy protections by regulations and courts. For example, although Part 2 (and similar state laws) allows disclosure of patient information to health information exchange organizations (HIOs),[75] some entities (including correctional institutions) might perceive the process of developing compliant policies and technical requirements as prohibitively complicated and choose not to participate. (In general, Part 2 programs would need to ensure that either patient consent or a qualified service organization agreement is in place in order for the program to disclose information to an HIO. In addition, patient consent would be needed for the HIO to redisclose the information to other specified HIO members, and any disclosures must be accompanied by a notice explaining the general prohibition on redisclosure.)

Furthermore, because most disclosures under Part 2 require detailed written consent, exchange organizations would be required to verify existence of the consent in addition to managing the information exchange. It is therefore possible that these entities will choose to exclude data covered by Part 2 or the provider institutions that contribute such data to avoid complex requirements and potential legal breaches. Similar issues are raised by state health information disclosure laws that require consent for disclosure of other types of health information (e.g., HIV, mental health).

Segmentation or sequestering of "sensitive" health information might offer a path forward that enables electronic exchange of the information and ensures its protection and compliance with privacy law in both the correctional environment and the community at large. 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.[76]

For example, when a substance abuse treatment program is part of a larger entity with multiple departments generating data for the same patient, data segmentation might enable exchange of certain elements in that patient's record without violating Part 2's requirements for disclosure.

Data segmentation could also be used to help patients express their preferences regarding information sharing, thereby supporting underlying principles of personal autonomy as well as enhancing patient trust and encouraging patient engagement.[76] Along these lines, the US Department of Health and Human Services is currently leading an initiative that supports pilot projects that allow providers to share portions of an EHR while not sharing others, such as information related to substance abuse treatment.[77]

Other methods of facilitating electronic health information sharing while appropriately protecting patient privacy are also being explored. For example, the Department of Health and Human Services has released guidance indicating that Part 2 would allow the use of single consent forms for multiple disclosures as well as multiple-party consent forms, methods that could be used in the correctional setting as well as the community. A single consent form could be used to authorize disclosure about a patient to one recipient, such as an HIO, and simultaneously authorize that recipient to redisclose the information to additional entities (e.g., other affiliated health care providers identified in the consent form) provided that the purpose for the disclosure is the same.

In addition, if a patient wished to authorize certain members of an HIO to access his or her Part 2–protected record as well as exchange information with one another, a multiple-party consent form could be developed that includes the names of each organization or person 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, a statement prohibiting redisclosure must accompany the information so that each subsequent recipient of the information is notified of Part 2's prohibition on redisclosure.[75]

Within the correctional environment, jurisdictions have developed ways to facilitate health information sharing based on individualized local circumstances, including state law, that could be adapted to the electronic environment as use of health information technology proliferates. These processes include locating criminal justice and mental health practitioners in the same facilities for ease of communication, developing procedures to obtain permission forms or court orders, contracting with business associates and qualified service organizations, and developing tools such as uniform authorization and consent forms and standard judicial orders. Inmates can complete authorization or consent forms at various stages in the criminal justice process, such as during the booking process in a jail or when they join 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 a collaborative system, allowing the individual to choose among them, provided that the special requirements for Part 2 consents are followed closely.[78]

CONCLUSIONS

Although expanding the use of health information technology in corrections has not been a major focus of state or federal policymakers to date, the use of EHRs does seem to be slowly increasing, and some local jurisdictions have explored different means of implementing health information technology connectivity. Such ventures have succeeded where, for example, jail connectivity is the community health mission of a public health department, part of a county initiative to improve reentry, or part of an external movement to strengthen the continuum of care in a community. These grassroots efforts depend on a confluence of policy factors, resources, and local champions for their success[26] and indicate that education of correctional health care providers and officials might be at least as instrumental in improving inmate health records and health care as legislative or administrative action.

The potential of health information technology in the inmate population is clear: the opportunity 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, both within the correctional environment and upon reentry into the community. The widespread use of EHRs and, eventually, electronic exchange in the correctional environment with appropriate privacy and security policies in place could play an important role in helping stabilize the health care of inmates while in correctional institutions as well as help ease their reentry into the community. ■

About the Author

Melissa M. Goldstein is with the Department of Health Policy, George Washington University School of Public Health and Health Services, Washington, DC.

Correspondence should be sent to Melissa M. Goldstein, JD, Department of Health Policy, School of Public Health and Health Services, George Washington University, 950 New Hampshire Ave NW, Suite 200, Washington, DC 20052 (e-mail: mgoldste@gwu.edu). Reprints can be ordered at http://www.ajph.org by clicking on the "Reprints" link.

This article was accepted December 10, 2013.

Acknowledgments

I gratefully acknowledge the support of Community Oriented Correctional Health Services, a nonprofit organization established to build partnerships between jails and community health care providers, and the Robert Wood Johnson Foundation in the preparation of a working draft of this article (available at http://cochs.org/library/HIE_CONF_ISSUE_PAPERs) prepared for an April 2012 conference on integrating jails into health information exchanges.

Human Participant Protection

No protocol approval was necessary because no human participants were involved.

References

1. Pub L No. 111-5, §§ 13001–13424 (2009).

2. Goldstein MM, Rein AL. Consumer consent options for electronic health information exchange: policy considerations and analysis. Available at: http://www.healthit.gov/sites/default/files/privacy-security/choice-model-final032610.pdf. Accessed January 23, 2014.

3. Pew Charitable Trusts. One in 100: behind bars in America 2008. Available

at: http://www.pewstates.org/research/reports/one-in-100-85899374411. Accessed January 23, 2014.

4. Minton TD. Jail inmates at midyear 2012: statistical tables. Available at: http://www.bjs.gov/index.cfm?ty=pbdetail&iid=4655. Accessed January 23, 2014.

5. Freudenberg N. Jails, prisons, and the health of the urban populations: a review of the impact of the correctional system on community health. *J Urban Health.* 2001;78(2):214–235.

6. Committee on Causes and Consequences of High Rates of Incarceration, Committee on Law and Justice, Division of Behavioral and Social Sciences and Education, Board on the Health of Select Populations, Institute of Medicine. Health and incarceration: a workshop summary. Available at: http://www.nap.edu/openbook.php?record_id=18372. Accessed January 23, 2014.

7. Williams BA, Stern MF, Mellow J, Safer M, Greifinger RB. Aging in correctional custody: setting a policy agenda for older prisoner health care. *Am J Public Health.* 2012;102(8):1475–1481.

8. Binswanger IA, Krueger PM, Steiner JF. Prevalence of chronic medical conditions among jail and prison inmates in the USA compared with the general population. *J Epidemiol Community Health.* 2009;63(11):912–919.

9. Wilper AP, Woolhandler S, Boyd JW, et al. The health and health care of US prisoners: results of a nationwide survey. *Am J Public Health.* 2009;99(4):666–672.

10. Hammett TM. HIV/AIDS and other infectious diseases among correctional inmates: transmission, burden, and an appropriate response. *Am J Public Health.* 2006;96(6):974–978.

11. Ludwig A, Cohen L, Parsons A, Venters H. Injury surveillance in New York City jails. *Am J Public Health.* 2012;102(6):1108–1111.

12. James DJ, Glaze LE. *Mental Health Problems of Prison and Jail Inmates.* Washington, DC: Bureau of Justice Statistics; 2006.

13. Steadman HJ, Osher FC, Robbins PC, Case B, Samuels S. Prevalence of serious mental illness among jail inmates. *Psychiatr Serv.* 2009;60(6):761–765.

14. US Department of Justice, Bureau of Justice Statistics. Substance dependence, abuse, and treatment of jail inmates, 2002. Available at: http://www.bjs.gov/index.cfm?ty=pbdetail&iid=1128. NCJ 209588. Accessed January 23, 2014.

15. Conklin TJ, Lincoln T, Wilson DR. *A Public Health Manual for Correctional Health Care.* Ludlow, MA: Hampden County Sheriff's Department; 2002.

16. Veysey B. *The Intersection of Public Health and Public Safety in US Jails: Implications and Opportunities of Federal Health Care Reform.* Oakland, CA: Community Oriented Correctional Health Services; 2011.

17. Damberg CL, Shaw R, Teleki SS, Hiatt L, Asch SM. A review of quality measures used by state and federal prisons. *J Correct Health Care.* 2011;17(2):122–137.

18. US Department of Justice. FY 2013 performance budget congressional submission: salaries and expenses. Available at: http://www.justice.gov/jmd/2013justification/pdf/fy13-bop-se-justification.pdf. Accessed January 23, 2014.

19. Texas curbs spending by $1B by deploying EHRs, telehealth in prisons. Available at: http://www.ihealthbeat.org/articles/2011/8/26/texas-curbs-spending-by-1b-by-deploying-ehrs-telehealth-in-prisons.aspx. Accessed January 23, 2014.

20. Bowman D. Telemedicine and EHR use for inmates helps save state $1B. Available at: http://www.fierceemr.com/story/ehr-use-inmates-helps-save-state-1b/2011-08-25. Accessed January 23, 2014.

21. Woodard A. Data tech can lower prison expense. Available at: http://www.ajc.com/opinion/data-tech-can-lower-1069305.html. Accessed January 23, 2014.

22. McGee MK. Philadelphia to roll out EHR from eClinicalWorks. Available at: http://www.informationweek.com/healthcare/electronic-medical-records/philadelphia-to-roll-out-ehr-from-eclini/229500696. Accessed January 23, 2014.

23. Wingett Y, Hensley JJ. In wake of suits, Maricopa County tackles jail-inmate care. Available at: http://www.azcentral.com/community/phoenix/articles/2010/05/11/20100511maricopa-county-jail-inmate-care.html. Accessed January 23, 2014.

24. Versel N. Los Angeles County approves $17M for EMR in juvenile detention facilities. Available at: http://www.fierceemr.com/story/l-county-approves-17m-emr-juvenile-detention-facilities/2010-06-03. Accessed January 23, 2014.

25. Community Oriented Correctional Health Services. Criminal justice and health information technology: what are the next steps? Available at: http://www.cochs.org/files/CJ_and_HIT_Roundtable-Proceedings.pdf. Accessed January 23, 2014.

26. Butler B. Jails and health information technology: a framework for creating connectivity. Available at: http://www.cochs.org/library/jails-health-information-technology-framework-creating-connectivity. Accessed January 23, 2014.

27. Goldstein MM. Health information technology and the idea of informed consent. *J Law Med Ethics.* 2010;38(1):27–35.

28. *Standards for Health Services in Jails.* Chicago, IL: National Commission on Correctional Health Care; 2008.

29. American Public Health Association Task Force on Correctional Health Care Standards. *Standards for Health Services in Correctional Institutions.* 3rd ed. Washington, DC: American Public Health Association; 2003;7.

30. American Bar Association. Standards for criminal justice: treatment of prisoners. Available at: http://www.americanbar.org/publications/criminal_justice_section_archive/crimjust_standards_treatmentprisoners.html#23-6.11. Accessed January 23, 2014.

31. Pinta ER. Decisions to breach confidentiality when prisoners report violations of institutional rules. *J Am Acad Psychiatry Law.* 2009;37(2):150–154.

32. Rothstein M. Currents in contemporary bioethics: constitutional right to informational health privacy in critical condition. *J Law Med Ethics.* 2011;39(2):280–284. [Citing Whalen v. Roe, 429 U.S. 589 (1977)].

33. Cohen F. No medical records privacy for inmate in sexual predator commitment proceeding. *Correctional Law Reporter.* 2010;22(3):35. [Citing Seaton v. Mayberg, 610 F.3d 530 (9th Cir. 2010); Doe v. Delie, 257 F.3d 309, 311 (3d Cir. 2011); Powell v. Schriver, 175 F.3d 107, 112 (2d Cir. 1999)].

34. Gostin LO, Burris S, Lazzarini Z. The law and the public's health: a study of infectious disease law in the United States. *Columbia Law Rev.* 1999;99(1):59–128.

35. Consumer Partnership for eHealth. Protecting sensitive health information in the context of health information technology. Available at: http://www.nationalpartnership.org/site/DocServer/Sensitive-Data-Final_070710__2_.pdf?docID=7041. Accessed January 23, 2014.

36. 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. Available at: http://www.iom.edu/~/media/Files/Activity%20Files/Research/HIPAAandResearch/PrittsPrivacyFinalDraftweb.ashx. Accessed January 23, 2014.

37. 45 CFR §160.103.

38. US Department of Health and Human Services. Standards for privacy of individually identifiable health information: proposed rule. *Fed Regist.* 1999;64(212):59918–60065.

39. US Department of Health and Human Services. Standards for privacy of individually identifiable health information: final rule: preamble. *Fed Regist.* 2000;65(250):82462–82829.

40. 45 CFR Part 160.

41. 45 CFR Part 164, Subparts A and E.

42. 45 CFR §160.203.

43. 45 CFR §164.502(a).

44. 45 CFR §164.502(a)(2).

45. 45 CFR §164.502(a)(1).

46. 45 CFR §164.508(a).

47. 45 CFR §164.506(a).

48. 45 CFR §164.512(e).

49. 45 CFR §164.512(f).

50. 45 CFR §164.512(j).

51. 45 CFR §164.512(k)(5).

52. 45 CFR §162, Subparts J–R.

53. Centers for Medicare and Medicaid Services. Covered entity charts. Available at: http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/downloads/coveredentitycharts.pdf. Accessed January 23, 2014.

54. Bizzell WD. The protection of inmates' medical records: the challenge of HIPAA privacy regulations. Available at: http://www.corrections.com/articles/11103-the-protection-of-inmates-medical-records-the-challenge-of-hipaa-privacy-regulations. Accessed January 23, 2014.

55. 45 CFR §164.501.

56. 45 CFR §164.520(a).

57. 45 CFR §164.524(a).

58. Pub L No. 91-616, 84 Stat 1848.

59. Pub L No. 92-255, 86 Stat 65.

60. 42 CFR §2.11.

61. 42 CFR §2.12(e)(1).

62. 42 CFR §2.31.

63. 42 CFR §2.12.

64. 42 CFR §2.51.

65. 42 CFR §2.53.

66. 42 CFR §2.52.

67. 42 CFR §2.32.

68. 42 CFR §2.20.

69. Pritts J, Lewis S, Jacobson R, Lucia K, Kayne K. Privacy and security solutions for interoperable health information exchange: report on state law requirements for patient permission to disclose health information. Available at: http://www.healthit.gov/sites/default/files/disclosure-report-1.pdf. Accessed January 23, 2014.

70. 42 CFR §2.64.

71. 42 CFR §2.65(d).

72. 42 CFR §2.65(e)

73. Snavely KR, Taxman FS, Gordon S. Offender-based information sharing: using a consent-driven system to promote integrated service delivery. In: Pattavina A, ed. *Information Technology and the Criminal Justice System.* Thousand Oaks, CA: Sage Publications; 2005:195–219.

74. 42 CFR §2.35.

75. Substance Abuse and Mental Health Services Administration. Applying the substance abuse confidentiality regulations to health information exchange. Available at: http://www.samhsa.gov/healthprivacy/docs/EHR-FAQs.pdf. Accessed January 23, 2014.

76. Goldstein MM, Rein AL. Data segmentation in electronic health information exchange: policy considerations and analysis. Available at: http://www.healthit.gov/sites/default/files/privacy-security/gwu-data-segmentation-final.pdf. Accessed January 23, 2014.

77. Data segmentation for privacy charter and members. Available at: http://wiki.siframework.org/Data+Segmentation+for+Privacy+Charter+and+Members. Accessed January 23, 2014.

78. Petrila J, Fader-Towe H. Information sharing in criminal justice–mental health collaborations: working with HIPAA and other privacy laws. Available at: http://csgjusticecenter.org/cp/publications/information-sharing-in-criminal-justice-mental-health-collaborations. Accessed January 23, 2014.