HEALTH

THE ARTS
CHILD POLICY
CIVIL JUSTICE
EDUCATION
ENERGY AND ENVIRONMENT
HEALTH AND HEALTH CARE
INTERNATIONAL AFFAIRS
NATIONAL SECURITY
POPULATION AND AGING
PUBLIC SAFETY
SCIENCE AND TECHNOLOGY
SUBSTANCE ABUSE
TERRORISM AND HOMELAND SECURITY
TRANSPORTATION AND INFRASTRUCTURE
WORKFORCE AND WORKPLACE

This PDF document was made available from www.rand.org as a public service of the RAND Corporation.

Jump down to document

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world.

Support RAND

Browse Books & Publications

Make a charitable contribution

For More Information

Visit RAND at www.rand.org

Explore RAND Health

View document details

This product is part of the RAND Corporation reprint series. RAND reprints reproduce previously published journal articles and book chapters with the permission of the publisher. RAND reprints have been formally reviewed in accordance with the publisher's editorial policy.

Michael D. Greenberg
M. Susan Ridgely
Douglas S. Bell

Electronic Prescribing and HIPAA Privacy Regulation

Electronic prescribing offers the prospect of safer medication management, but fulfillment of that promise depends on ready access to personal health information from many sources, thus raising new concerns about information privacy and security. Federal privacy regulations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) limit the sharing of health information by providers, and particularly may discourage information sharing over distributed computer networks. This analysis finds that although HIPAA has only a limited effect on current e-prescribing practices, future electronic prescribing systems will likely fall short of their potential benefits, absent policy refinements designed to encourage clinically appropriate, networked sharing of patient health information.

The public health effects of new drugs depend in part on their being accurately and appropriately prescribed. Prescribing, however, has only recently started to undergo a high-technology shift analogous to the transformation of medicine more generally. The proliferation of networked information systems promises a new dimension for innovation in health care, with pharmacy and the medication management process presenting a prime target for reform (DHHS 2000; NAS 2000).

In the abstract, electronic prescribing ("e-prescribing" or "e-Rx") involves the use of computerized technologies to support the writing and verification of prescriptions, the dispensing of medications to patients, and the maintenance of related records, potentially across multiple physical locations and medical providers. Electronic prescribing systems could offer numerous advantages over pen and ink, including automated screening for contraindications, the integration of prescriptions into an electronic medical record, and reduction of communication errors between health care providers and pharmacists (Bell et al. 2004). At the same time, the conversion of medical information (including prescriptions) to a digital medium also creates new potentials for misappropriation and breach of confidentiality. Fueled in part by these concerns, the U.S. Congress passed the Health Insurance Portability and Accountability Act of 1996 (HIPAA), thereby authorizing federal regulations to establish privacy and security safeguards for identifiable health information (HIPAA 1996). With regard to prescribing practice, these regulatory safeguards are important because they impose on

Michael D. Greenberg, J.D., Ph.D., *is an associate behavioral scientist at RAND Health in Pittsburgh, Pa.* ***M. Susan Ridgely, J.D.,*** *is a senior policy analyst at RAND Health in Santa Monica, Calif.* ***Douglas S. Bell, M.D., Ph.D.,*** *is an assistant professor, Division of General Internal Medicine and Health Services Research, David Geffen School of Medicine at University of California, Los Angeles.* *Support for this research came from Pfizer, Inc.* *Address correspondence to Dr. Greenberg at RAND Health, 201 North Craig St., Pittsburgh, PA 15213. Email: michael_greenberg@rand.org*

Inquiry 41: 461–468 (Winter 2004/2005). © 2004 Excellus Health Plan, Inc.
0046-9580/04/4104–0461

physicians and pharmacists the affirmative obligation to protect prescription information from misuse or wrongful disclosure. The safeguards are also likely to influence the development of future electronic prescribing systems by introducing privacy and security standards into e-Rx system design, and by limiting the functions such systems may perform.

This paper examines the practical impact and policy implications of federal privacy and security regulations under HIPAA for electronic prescribing. By now, HIPAA and its regulations have become widely known, in part because of the strenuous compliance efforts that providers and health plans have been forced to undertake. Many academic and professional commentaries already have been written on HIPAA and its legal requirements (see e.g., Annas 2003; Hussong 2000; Ridgely and Greenberg 2002). Rather than recapitulating a full summary of those requirements here, we assume that readers are already familiar with the basic HIPAA regulatory scheme, and we address only those specific elements of the regulations that raise greatest concern for e-prescribing. In our view, the effect of federal HIPAA regulations, although placing a significant burden on prescribing practice generally, probably does not impose much incremental burden on current forms of electronic prescribing over conventional practice. However, the HIPAA regulations do raise a flag of concern for future development of new e-Rx systems. The HIPAA regulations are likely to have an inhibitory effect on the networked sharing of personal health information among providers, which could undercut the potential clinical benefits that technology might bring to new e-Rx systems.

The development of new e-Rx systems ultimately reflects two sets of competing interests. On the one hand, privacy rights for consumers entail administrative burdens for health care providers and limits on providers' ability to use and disclose patient information. On the other hand, future innovations in prescribing technology could help to transform the practice of medicine, and perhaps to improve radically the safety of patients. But the necessary technical innovations could require building a distributed information infrastructure for prescriptions, as well as broadband sharing of prescription information among clinical providers. It is not clear that the privacy rules contemplate, or will permit, this kind of information sharing, and the result could be to impede the development of new technology with substantial value for patient care. The purpose of this paper is to elucidate the trade-off, and ultimately to suggest ways in which the balance of interests between privacy and new e-Rx technology might be refined to the benefit of consumers.

HIPAA Privacy Regulations: Core Concepts

At their most general level, the federal privacy rules under HIPAA can be understood as creating broad nondisclosure responsibilities for medical providers, health plans, and health care clearinghouses (collectively, "covered entities"), in connection with health information that includes patient identifiers (i.e., protected health information or PHI). With regard to such information, covered entities are not only prohibited from making disclosures, but also have the affirmative obligation to protect against unauthorized use or access—an obligation that takes the form of technical, administrative, and physical requirements to ensure information security. Against this broad set of privacy requirements, the HIPAA rules establish a series of exemptions, within which the use and disclosure of PHI is permitted. The most important of these safe harbors covers "treatment, payment, and operations" (TPO), and allows for the use of protected information by clinicians in actually delivering health care to a patient. Conventional prescribing activities would ordinarily fall within this TPO safe harbor, although providers of care nevertheless remain bound to honor the safeguarding requirements of the privacy rules.

Current Effects of HIPAA Privacy Rules on E-Rx Practice Similar to Conventional Rx

As of 2004, some forms of electronic prescribing have already begun to proliferate among American health care providers. Fax-based transmission of prescriptions, for example, is fairly widespread, and an initial generation of e-prescribing digital technologies (e.g., using palm-top computers and Internet-based communications) also have been tested and deployed in various parts of the country (Ash, Gorman and Hersh 1998). Current e-Rx systems involve the use of computers to

facilitate prescription data entry, storage of prescription information, and transmission of related data between physicians and pharmacists. This kind of e-Rx activity broadly falls into the TPO regulatory exemption under HIPAA (DHHS 2004a, 2004b) – that is, activity in direct service of clinical care. Consistent therewith, the use and disclosure of personal health information in connection with e-prescribing can generally be undertaken by providers without written authorization from individual patients. Nevertheless, HIPAA privacy and security standards still exert influence over several aspects of the prescribing process, including storage of and access to related records, as well as the communication of records between providers. Note that HIPAA is not restricted in its application to protected health information in digital form (DHHS 2004c). As a result, some elements of the HIPAA regime apply to all prescribing activities (whether or not e-Rx technology is involved), while others apply specifically to e-Rx transmissions and to the computer systems in which digital prescription information resides.

Some of the broader privacy mandates under HIPAA require the protection of PHI through limitations on information access to appropriate health care personnel, physical safeguarding of information (or information systems) against unauthorized intrusion, training of personnel with regard to appropriate privacy procedures, and limitation of nontreatment disclosures of PHI to a "minimum necessary" standard (see general discussion and regulatory citations in Ridgely and Greenberg 2002). Notably, these sorts of requirements impose similar demands on prescribing physicians and pharmacists regardless of whether e-Rx systems are adopted in support of clinical practice. PHI, even when reduced to a physical paper record, is entitled to these protections. As a practical result, physicians and pharmacists generally have had to tighten controls over PHI in prescription records across a range of clinical settings, and have had to ensure that support staff are both familiar and compliant with privacy procedures (DHHS 2004d).

The adoption of new technology to support prescribing (particularly in electronic record keeping) in no way modifies these HIPAA standards. But because electronic records are more portable and more readily duplicated than paper, HIPAA regulations also impose some additional security burdens on electronic media, primarily in the form of technical access controls and user authentication features (like password protection; DHHS 2004e). Given that these sorts of technical features have to be incorporated into the design of e-Rx software, it is not clear that they create a disincentive to electronic prescribing per se, apart from any associated incremental costs for the acquisition of e-Rx systems.

The element of the prescribing process that most implicates privacy concerns involves the transmission of information between physicians and pharmacists. Clinically, this transmission is important because it defines the nature of the medication to be dispensed to the patient, and because it involves a collaboration between physician and pharmacist to ensure medication appropriateness and safety. From a privacy perspective, the transmission of prescriptions is also important, in part because information in transit is subject to unlawful interception, and in part because information once transmitted should retain the same level of privacy protection that it held originally. Old-fashioned written and telephone prescriptions implicitly involve an authentication process, either through direct contact between doctor and pharmacist, or through the formal identification provided by a signed prescription blank. Authentication serves a number of functions unrelated to privacy; among other things, it helps to ensure that both professional parties involved in a prescription are bound by HIPAA privacy rules, and are legitimately engaged in clinical activity within the TPO exemption. By implication, both physicians and pharmacists have an obligation to protect against unlawful intrusion on the prescription process. Where Rx communications are paper- or telephone-based, the risks of intrusion are partly mitigated by the nature of the communications medium, which is fundamentally less amenable to misappropriation than is digital communication.

E-Rx technologies that support the transmission of digital prescriptions create incremental privacy and security burdens beyond those that apply to more conventional communications. Authentication of digital prescriptions, for example, requires technical support through features in e-Rx software, since digital prescriptions involve no direct contact between professionals, and no physical signatures from doctors.[1] HIPAA

privacy and security rules include these sorts of technical requirements for electronic interchanges of PHI, and even contemplate the development of new authentication technologies such as digital signatures (DHHS 2004e). Likewise, the electronic communications medium itself raises more concerns about security and misappropriation than does conventional communication, because electronic records are inherently easier than paper to copy and to transmit. As a result, HIPAA privacy and security rules establish computerized standards for protecting information in transit, as by encrypting data and limiting outside access to communications nodes that store PHI (DHHS 2004e). Although these sorts of requirements do impose an incremental technology burden on the development of e-Rx systems, it is again unclear that they create an operational disincentive to e-prescribing apart from incremental technology costs.

E-prescribing, in its simplest form, is limited to bilateral communications between a doctor and a pharmacist, and to ancillary tasks such as prescription data entry and record-keeping by both parties. Many of the restrictions that HIPAA imposes on this simple form of e-prescribing are no different from HIPAA restrictions that apply to pharmacy practice more generally. Moreover, to the extent that HIPAA standards entail unique requirements for e-prescribing, those burdens are largely manifested in technical privacy and security features in the design of e-Rx systems, rather than in operational burdens on the clinical practice of e-prescribing. In fact, it is difficult to identify new, specific HIPAA-related liability risks in prescribing practice—at least that accrue uniquely to the use of e-Rx technology in favor of traditional modes of communication. One possible example of such risk might involve e-Rx systems that allow physicians to order prescriptions through a palm-top computer interface (i.e., PDA). Note that PDAs are inherently portable, and are potentially a desirable target for theft. To the extent that identifiable prescription data resides within an e-Rx PDA, then HIPAA regulations might foreseeably require doctors to take reasonable care in safeguarding their PDAs from theft, loss, or intrusion (DHHS 2004d). Once again, however, technical features in e-Rx systems could be designed to ameliorate PDA privacy risks, as by password protection, data encryption, and limiting the amount of PHI that is stored locally in a PDA interface. In sum, the effects of HIPAA on the simplest forms of bilateral e-Rx practice, while not insubstantial, are not qualitatively distinct from HIPAA's effects on conventional prescribing practice.

Future Effects of HIPAA Privacy Rules on E-Rx Development

Notwithstanding the previous discussion, HIPAA privacy and security rules nevertheless represent a significant constraint on e-prescribing systems and technology development. Much of the desirability of e-Rx technology lies not in its current limited incarnation, but rather in its future potential for transforming the prescribing process. From a clinical perspective, the writing of prescriptions is an important element in the broader management of a patient's care. Information about an individual's prescriptions could potentially be relevant to many different health care professionals, all of whom work in providing a range of clinical services to a patient. Conversely, good clinical decisions about prescribing medications also might draw on patient-care information from diverse health care settings, services, and professionals. Thus, although individual instances of prescription writing may be bilateral (i.e., occurring between one physician and one pharmacist), the Rx process is nevertheless embedded in a larger network of health care information, and ideally should draw on and distribute information to that network in support of clinical care. E-Rx technology has the potential to facilitate the networked flow of prescription information in a manner that is qualitatively different from the bilateral communication of prescriptions by paper or telephone.

Given the aforementioned, what kinds of technical features might be required for future e-Rx systems to achieve their full functional potential? A recent expert panel study led by RAND to develop standards for e-Rx systems offers some guidance for what e-Rx might optimally look like in the future (Bell, Marken et al. 2004). In particular, e-Rx systems could involve significant automated decision support tools to ensure appropriate prescribing practice, given available diagnostic, treatment, and insurance information for particular patients. Systems could generate alerts to prescribers in the event of medication contraindications or other possibilities for prescribing er-

ror. Systems also could be designed to monitor patient adherence to prescriptions, to provide prescribers with related information about adherence and renewals, and to give automatic reminders and tracking concerning related laboratory test information. One of the key requirements that underlies these sorts of functions involves the capacity of e-Rx systems to integrate with other sorts of health care information technologies, including electronic medical records and practice management databases. This kind of integration could permit e-Rx systems to access patient historical data from a range of medical and pharmacy sources, and allow these systems to generate both a current prescription list and a complete prescription history. Security features presumably would be included in e-Rx systems to restrict data access to those physicians, pharmacists, and support staff who have clinical responsibility with regard to specific patients.

The kind of system integration and data sharing that offers greatest promise for improving clinical prescribing practice is also the most challenging aspect of e-Rx under HIPAA and the privacy regulations. As discussed earlier, e-Rx in its simplest, bilateral form is a basic aspect of clinical health care, and as such falls within the TPO exemption under the HIPAA privacy rules. Electronic prescribing in the context of a distributed health information infrastructure, however, is another animal. E-Rx systems that generate and share information across multiple provider organizations and pharmacies create a range of privacy and security concerns that go well beyond the simple bilateral case. This occurs in part because access to prescription information cuts across multiple organizations and computer platforms, and in part because individual health care organizations have diminished control over information in a distributed network.

The threshold legal question that arises here is whether this kind of distributed e-Rx activity still falls within the TPO exemption as an aspect of clinical care, or whether the networked maintenance and exchange of prescription information goes beyond the scope of the TPO exemption. The answer to this question is ambiguous under the HIPAA privacy regulations — arguments could be advanced to support either conclusion. Regardless, what is apparent is that advanced e-Rx technology could involve massive sharing and processing of clinical data across computer networks in a manner that is different from conventional clinical care, but which arguably might supplement or replace it.

If the TPO exemption does not apply, then distributed e-Rx information sharing would have to be shoe-horned into HIPAA compliance through some other regulatory mechanism, perhaps under the business associate rule. But even if the TPO exemption *does* apply, the exchange and maintenance of prescription information in a distributed, inter-organizational computer network still raise significant questions under HIPAA. The HIPAA privacy rules, for example, establish that patients have a right not only to review their health care records, but to demand the correction of mistakes (DHHS 2004f; DHHS 2004g).

It is not clear how these rules would apply in a context of an e-Rx infrastructure where no single organization has control over prescription records, and where every organization depends on information that is supplied and maintained by others. Similarly, one might ask how the privacy notice requirements under HIPAA (DHHS 2004h) are supposed to apply in circumstances where the privacy of prescription information is as much affected by *other* organizations' privacy policies as by those of a specific pharmacy or medical practice. One also might raise the question whether, and to what extent, any single provider in an e-Rx network assumes responsibility for the privacy and security measures undertaken by other participants in a distributed network. Note that prescription information, once generated by a clinician, should retain its fundamental privacy and security protections after entering an e-Rx network: HIPAA does not specify any "due diligence" requirements for providers who participate in this kind of e-Rx information exchange, likely because the federal regulations were not written in contemplation of the development of this kind of health information network.

An exhaustive listing of the ways in which HIPAA rules (and ambiguities) might impact future e-Rx systems goes beyond the scope of this paper. But there are two key points that deserve emphasis. First, criminal and administrative liability under HIPAA creates substantial incentives for compliance with the privacy rules.[2] To the extent that the rules are ambiguous in interpretation, draconian liability would presumably motivate providers and pharmacists to err on the side of conservatism in regard to their privacy

policies, and consequently, in their adoption of new information technologies. Second, the development of new e-Rx systems presumably will be influenced by the contours of professional responsibility and liability established under HIPAA. To the extent that providers are either unable or unwilling, because of HIPAA, to exchange PHI over networks in support of clinical care, then the design of future e-Rx systems is likely to fall short of supporting some of the kinds of network-based clinical features described earlier. Ultimately, the concern is that HIPAA's regulations and ambiguities could impede the development of e-Rx technology in ways not foreseen by regulators, thereby undermining the utility of e-Rx as a device for promoting patient safety in medication management.

Discussion

The impact of HIPAA on the development of new e-Rx technology is both subtle and far-reaching. The HIPAA privacy regulations are complicated and ambiguous in themselves, notwithstanding the continuing efforts of federal officials to provide guidance and clarification (DHHS 2004i). The impact of the law on e-Rx will depend, over time, on how the law is interpreted by regulators, courts, and state authorities. The ambiguity in the HIPAA rules is compounded by state privacy laws, and particularly state tort actions, which might adopt HIPAA standards as a platform for establishing civil liability against violators. The interface among HIPAA privacy rules, state tort laws, and future e-Rx technologies that have not yet been developed is necessarily speculative. Nevertheless, what is clear is that HIPAA and other health privacy laws will need to be interpreted and applied to a kind of distributed computing not presently commonplace in clinical health care. Under some interpretations, HIPAA rules and ancillary state privacy laws could create significant barriers to the development of this sort of technology. Thus, intervention by policymakers may be required to ensure that e-Rx and related technologies fully achieve their potential benefits.

Setting privacy concerns aside, it is noteworthy that e-Rx technology already has become an important element in several recent health care policy initiatives. Government efforts to address a perceived crisis in patient safety, for example, have included a focus on the development of new clinical information technologies, including e-prescribing and computerized physician order entry (CPOE) systems (AHRQ 2004). Public investment in these technologies reflects a conviction among health policymakers that the technology can help to alleviate systemic errors in health care settings, with significant benefits to consumers and to society as a whole. In a complementary vein, recent Medicare legislation also has pressed the development of e-prescribing, by creating a grant program supporting the implementation and adoption of e-Rx technology starting in 2007 (Medicare Prescription Drug and Modernization Act of 2003, §108). Incongruously, these sorts of policy initiatives to promote e-Rx and its benefits could be undercut by HIPAA and other privacy laws, at least to the extent that network-based e-Rx functions are limited or curtailed. Resolution of the conflict will require a broader focus by policymakers on the legal landscape that surrounds e-Rx, and not just on government technology mandates and subsidy programs.

Again, it is important to acknowledge that privacy regulations under HIPAA reflect a balance among competing policy goals. Previous commentators have suggested that there is a fundamental trade-off between consumer privacy interests, and technology-enabled improvements in patient safety and health care quality (Gostin 1995). Without commenting on the relative importance of these interests, society would clearly be better off with policy reforms that facilitate the development of new e-Rx technologies, while simultaneously preserving rigorous privacy protections. This paper has argued that current federal privacy rules are likely to deter the development of e-Rx technologies in ways not easily foreseeable to the original authors of HIPAA. In consequence, future policy reform efforts should focus initially on ameliorating HIPAA disincentives to the development of new e-Rx systems, consonant with maintaining optimal privacy rights for consumers. At the margin, however, policymakers eventually may need to re-examine the appropriate balance between privacy interests and patient safety given the potential benefits that e-Rx, and other transformational medical technologies, might bring.

What are some specific recommendations for reform in connection with HIPAA and e-Rx?

First, policymakers should revise and clarify federal rules to recognize explicitly that networked information exchange in support of clinical practice is permitted under the TPO safe harbor of HIPAA. Participating in an e-Rx information network should not, by itself, violate the law, nor should participating make clinicians liable for privacy violations committed by other network participants. At the same time, the HIPAA privacy rules also may need revision to ensure adequate security, validation, and consumer opt-out measures in connection with access to distributed health information networks. The ultimate goal of reform is not to emasculate HIPAA, but instead to obtain appropriate privacy protections while facilitating the development of fully functional, network-based e-Rx systems. Achieving this goal also could involve some marginal tailoring of federal pre-emption of state privacy laws. Although controversial, such reform might help to capture the benefits of a safer, technology-enabled health care system, while preserving core policy interests in health information privacy.

In sum, HIPAA privacy and security regulations do exert operational requirements on current electronic prescribing activities, but may have a more far-reaching impact on future e-Rx systems and activities. HIPAA has the potential for undercutting future development of e-Rx by creating disincentives to the adoption of new e-Rx systems by provider organizations, and by influencing the design of future e-Rx systems and the kinds of functions that such systems eventually will support. It is the latter effect that should be of focal concern to policymakers seeking to balance interests in patient safety, information privacy, and new forms of health information technology. In the absence of targeted reforms to current privacy laws, there is a significant likelihood that the potential benefits from e-Rx technology will not be fully realized.

Notes

1 Of course, a pharmacist could always telephone a physician to confirm the validity of an electronic prescription, but part of the functional benefit of e-Rx systems presumably involves eliminating the need for that kind of direct contact.

2 Civil liability under state tort laws (e.g., for breach of confidentiality) may also create incentives for compliance with HIPAA privacy standards.

References

Agency for Healthcare Research and Quality (AHRQ). 2004. Using Computers and Information Technology to Prevent Errors. Available at: http://www.ahrq.gov/qual/newgrants/it.htm Accessed Feb. 20.

Annas, G. J. 2003. HIPAA Regulations – A New Era of Medical-Record Privacy? *New England Journal of Medicine* 348(15):1486–1490.

Ash, J.S., P.N. Gorman, and W.R. Hersh. 1998. Physician Order Entry in U.S. Hospitals. *Proceedings of the American Medical Informatics Association*. pp. 235–239.

Bell, D.S., S. Cretin, R.S. Marken, and A.B. Landman. 2004. A Conceptual Framework for Evaluating Outpatient Electronic Prescribing Systems Based on their Functional Capabilities. *Journal of the American Medical Informatics Association* 11(1):60–70.

Bell, D.S., R.S. Marken, R.C. Meili, C.J. Wang, M. Rosen, R.H. Brook, and RAND Electronic Prescribing Expert Advisory Panel. 2004. Recommendations for Comparing Electronic Prescribing Systems: Results of an Expert Consensus Process. *Health Affairs*. Web exclusive. May 25. Available at: www.healthaffairs.org

Department of Health and Human Services (DHHS). 2000. Standards for Privacy of Individually Identifiable Health Information. *Federal Register* 65:82,461–82,465.

———. 2004a. 45 C.F.R. § 164.502, *Privacy of Individually Identifiable Health Information: Uses and Disclosures of Protected Health Information, General Rules*.

———. 2004b. 45 C.F.R. § 164.506, *Privacy of Individually Identifiable Health Information: Uses and Disclosures to Carry Out Treatment, Payment, or Health Care Operations*.

———. 2004c. 45 C.F.R. § 160.103, *General Administrative Requirements: Definitions*.

———. 2004d. 45 C.F.R. § 164.532, *Privacy of Individually Identifiable Health Information: Administrative Requirements*.

———. 2004e. 45 C.F.R. § 164.312, *Security Standards for the Protection of Electronic Protected Health Information: Technical Safeguards*.

———. 2004f. 45 C.F.R. § 164.524, *Privacy of Individually Identifiable Health Information: Access of Individuals to Protected Health Information*.

———. 2004g. 45 C.F.R. § 164.526, *Privacy of Individually Identifiable Health Information: Amendment of Protected Health Information*.

———. 2004h. 45 C.F.R. § 164.520, *Privacy of Individually Identifiable Health Information: Notice of Privacy Practices for Protected Health Information.*

Department of Health and Human Services (DHHS). Office for Civil Rights. 2004i. Medical Privacy – National Standards to Protect the Privacy of Personal Health Information. Available at: http://www.hhs.gov/ocr/hipaa/ Accessed Feb. 20.

Gostin, L. O. 1995. Health Information Privacy. *Cornell Law Review*. 80:451–528.

Health Insurance Portability and Accountability Act (HIPAA) of 1996. Pub. Law No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 42 U.S.C.).

Hussong, S. J. 2000. Medical Records and Your Privacy: Developing Federal Legislation to Protect Patient Privacy Rights. *American Journal of Law & Medicine* 26(4):453–474.

Medicare Prescription Drug and Modernization Act of 2003. Pub. Law No. 108-173, 117 Stat. 2066.

National Academy of Sciences (NAS). 2000. *Networking Health: Prescriptions for the Internet* Washington, D.C.: National Academy Press.

Ridgely, M.S., and M.D. Greenberg. 2002. Pharmacy, Facsimile and Cyberspace: An Examination of Legal Frameworks for E-Prescribing. *Albany Law Journal of Science and Technology* 13(1):1–42.