

White Paper
November 2006
© 2006 Christiansen IT Law
Licensed for distribution without
alteration and with attribution intact.

John R. Christiansen, J.D.
Christiansen IT Law
Privacy/Security/Compliance
2212 Queen Anne Avenue North #333
Seattle, Washington 98109
206.301.9412
john@christiansenlaw.net

USING SAFE HARBORS TO REDUCE LEGAL BARRIERS TO IMPLEMENTATION OF ELECTRONIC HEALTH RECORDS AND HEALTH INFORMATION NETWORKS

This white paper proposes that state governments should take a leadership role in reducing legal barriers to electronic health record (EHR) and health information network (HIN) adoption, by implementing a regulatory “safe harbors” scheme for EHR and HIN privacy and security policies and practices. Model EHR and HIN safe harbors legislation is provided in Appendix A, and demonstration regulations are provided in Appendix B.

Since this white paper is intended as a “straw man” to advance discussion of solutions to legal barriers – real and perceived – to EHR and HIN implementation, it does not include comprehensive legal analysis or legal citations. It does assume the reader is generally familiar with EHR and HIN issues, the privacy and security requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and comparable state law principles, and to some extent with regulatory processes.

Introduction.

The lack of clear legal standards for EHR and HIN privacy and security is perhaps the fundamental legal obstacle to their widespread adoption. In their absence healthcare organizations don’t know what they have to do to avoid possible regulatory penalties and civil liabilities. Uncertainty always weighs against action, especially when the uncertainty concerns legal risks.

While some of this uncertainty could probably be resolved by minimal research and analysis, some of it is legitimate and inevitable given the current state of the law. The solution is therefore to develop legal certainty to the extent possible, at least for key privacy and security issues.

**USING SAFE HARBORS TO REDUCE LEGAL BARRIERS TO IMPLEMENTATION OF
ELECTRONIC HEALTH RECORDS AND HEALTH INFORMATION NETWORKS**

November 2006

In principle this might be done by legislative mandate, but that is a blunt and inflexible instrument badly suited to emerging technology issues. Over time it might also be developed by common law, through litigation; but that would take many years at best, and the risk of litigation is itself part of the current problem.

Legal certainty is therefore more readily developed through a regulatory “safe harbors” solution. This kind of solution has been implemented for comparable problems in a number of areas, including the confusing and problematic field of healthcare financial “fraud and abuse” (the so-called “Stark” and “antikickback” laws), which provides a useful model for EHR and HIN safe harbors.

One solution to this might be federal safe harbors, but it would probably take much longer to develop and pass federal implementing legislation and develop the necessary regulations than it would to do so at the state level. Quite apart from the more complex political logistics, it seems likely it would be much more difficult to identify nationally-acceptable policies and practices given the variations among the states. A state-based strategy would instead let states whose healthcare communities felt they were ready to implement safe harbors go forward, and allow the others to follow as they were ready.

A state-based approach does raise the potential problem of non-uniformity. One state’s safe harbors may not match those of its neighbors, or its neighbors may not implement or formally recognize safe harbors at all.

While this is a legitimate concern, the fact is that there is currently no legal mechanism for development of uniformity at all. Policies and business practices tend to be developed by standards bodies and professional organizations which are not legal authorities, and are implemented ad hoc by organizations which may or may not take standards bodies’ and professional organizations’ guidance into account. The implementation of safe harbors state-by-state should therefore tend to increase rather than decrease uniformity compared to the current situation, especially if states adopting safe harbors coordinate their regulations.

By the same token compliance for organizations operating across state lines should also become simpler. Since safe harbors compliance is by definition not mandatory, interstate organizations will be able to opt-out of safe harbors which are not appropriate. Perhaps more likely, organizations operating in both states with safe harbors and those without will opt to comply and get the benefit of the safe harbors where possible. Since states which are not ready for safe harbors are also unlikely to be ready to impose legal mandates which conflict with other states’ safe harbors, interstate organizations should be better able to implement consistent policies and practices across the organization.

**USING SAFE HARBORS TO REDUCE LEGAL BARRIERS TO IMPLEMENTATION OF
ELECTRONIC HEALTH RECORDS AND HEALTH INFORMATION NETWORKS**

November 2006

Uncertainties in EHR and HIN Privacy and Security Law.

There is no special legal domain for EHRs and HINs. An EHR is nothing more than a computer system used to receive, store, process and produce health information, and a HIN is any set of network technologies used to transmit it from computer system to computer system. However, the laws which apply to EHRs and HINs are the same which apply to health information in general: Principally HIPAA and a few other federal laws, plus the laws of whatever states the computer systems and the organizations which use them are located, and the individuals whose information is present in the EHR or HIN are residents.

While some requirements of these laws are fairly clear, at least with a little work, others are not. Since EHR and HIN implementation always requires changes to business practices, it is sometimes unclear how a privacy-related policy or practice should be adapted to new arrangements. Security requirements in particular are problematic, since these are almost universally risk-based and not prescriptive. In other words, they do not describe specific policies, practices or technologies which must be adopted, but require healthcare organizations to analyze security risks and make reasonable and appropriate decisions about the security safeguards they will implement.

It is therefore difficult and sometimes impossible to determine a priori whether many privacy policies and practices, and almost all security policies and practices, will be considered compliant with applicable law. This may be made somewhat clearer with a couple of examples.

On the privacy side, for example, a health care provider wishing to share health information using a HIN may be concerned whether this sharing needs to be disclosed to potentially affected patients. Under HIPAA and a number of state laws health care providers are required to give patients a notice of their privacy or information practices – that is, a general description of the ways they use or disclose patient information. However, none of these laws has any provision specifically applicable to HIN usage. The health care provider has no guidance, and must decide for itself whether HIN participation information should be included, and if so what the notice should say.

On the security side, the same provider may wonder what authentication processes it should implement for users of an EHR it is setting up. Its EHR vendor may suggest single-factor password authentication, a relatively inexpensive option. Its consultants, on the other hand, may suggest using two-factor authentication using both passwords and tokens or swipe cards, a more expensive option. While HIPAA and some state laws both indicate that some form of authentication must be implemented, they provide no guidance for choosing between single- and two-factor authentication; they simply tell the provider to do a risk analysis, and choose the “reasonable and appropriate” option.

**USING SAFE HARBORS TO REDUCE LEGAL BARRIERS TO IMPLEMENTATION OF
ELECTRONIC HEALTH RECORDS AND HEALTH INFORMATION NETWORKS**

November 2006

The degree to which this kind of uncertainty is acceptable depends on the provider's tolerance for risk. In principle, if the provider makes informed and reasonable determinations appropriate to its conditions and circumstances – if its privacy and security decision-making processes are adequate – it should not be liable if something goes wrong and health information is negatively affected. In practice, patients may be alarmed to discover that their information is being shared over a HIN and claim that the notice they received was inadequate; or in the event of an EHR security breach, may claim even two-factor authentication was inadequate.

While good decision-making practices *should* prevent legal liabilities in such cases, there is no assurance that they *will*. If there is some sort of harm to affected individuals, especially if there is a public outcry or media attention, judges, juries and even regulatory authorities may be inclined to try to find reasons to give the victims some kind of recourse. What seemed reasonable and appropriate at the time may, with the benefit of hindsight and adversarial scrutiny, come to seem unreasonable and negligent.

This kind of legal risk is a material obstacle to EHR and HIN implementation. Some organizations are comfortable with this level of legal risk, or perhaps don't notice it. Others have a lower tolerance for legal risk, perhaps especially when it is added to the operational and financial risks of new technology implementation in the first place.

To the extent that legal uncertainties about EHR and HIN standards and practices can be reduced, then, a material barrier to their implementation will be lowered for at least some organizations. And some of these uncertainties, at least, can be dealt with by the creation of safe harbors for key policies and practices.

Using Safe Harbors to Reduce Legal Uncertainty.

Safe harbors should be carefully distinguished from legal mandates. A legal mandate is a statute or regulation (or much more rarely caselaw) which prescriptively identifies a specific legal requirement, with penalties for its violation. For example, the HIPAA privacy regulations require publication of a notice of privacy practices, and prescribe its content with some specificity. An organization which is required to publish a privacy practices notice and fails to include content prescribed by the rules is subject to regulatory penalties, and possibly exposed to claims for damages by patients claiming to have been harmed by the failure.

A safe harbor, on the other hand, does not prescribe any requirements, nor is there a penalty for noncompliance. Rather, a safe harbor describes a set of facts and the policies and practices implemented by an organization under those facts, and states an agency's interpretation that under those facts the described policies and practices do not violate the applicable law. Organizations are not penalized for failing to implement those policies and procedures, but those which choose to do so are assured they will not be penalized. Organizations which choose not to do so have no such assurance, but are not necessarily in violation of applicable law and therefore not necessarily subject to penalties.

**USING SAFE HARBORS TO REDUCE LEGAL BARRIERS TO IMPLEMENTATION OF
ELECTRONIC HEALTH RECORDS AND HEALTH INFORMATION NETWORKS**

November 2006

A safe harbor therefore reduces legal risk, as opposed to a legal mandate which actually creates it. A safe harbor scheme would therefore reduce legal risks in EHR and HIN implementation, and so reduce this barrier to implementation, as opposed to legal mandates which would only raise it higher.

A safe harbor scheme can also accommodate the problematic issue of different and changing technologies and circumstances better than a legal mandate scheme. This problem is the legitimate reason why the HIPAA security regulations are risk-based rather than prescriptive: It takes much longer to change statutes than it does regulations, and longer to update regulations than to update regulatory guidance. Any specific prescriptive requirements would be at risk of becoming obsolete, and perhaps counter-productive, more quickly than they could be revised.

For this reason HIPAA itself – the legislation rather than the regulations usually identified with it – deliberately established a regulatory structure which authorized and directed agency issuance of appropriate regulations, to accommodate changing and variable needs and circumstances. The HIPAA enforcement regulations in turn establish a dispute resolution structure which includes publication of interpretive decisions to help guide healthcare organizations – though it appears it will be some time before a significant number of cases reaches that level.¹

This structure is not unique to HIPAA, and in fact is relatively well-developed in the healthcare “fraud and abuse” area. This is a field in which legislation established draconian penalties for violations of broad, confusing and counterintuitive laws. Given the breadth and difficulty of interpretation of these laws, a risk-averse interpretation would tend to rule out many legitimate and even beneficial business arrangements and transactions. In other words, the fraud and abuse laws created legal uncertainties which may be a material barrier to valuable activity.

In order to overcome this barrier, the U.S. Department of Health and Human Services publishes safe harbor regulations interpreting the fraud and abuse laws as applied to specific sets of facts.² Less formal guidance documents, as well as opinions on specific factual situations presented in letters requesting guidance, provide additional assurances which help reduce the risks to healthcare organizations seeking to develop business arrangements and transactions which they otherwise might avoid altogether – even when they might provide material benefits to patient care and administration.

¹ The U.S. Department of Health and Human Services does provide some interpretive guidance on HIPAA privacy issues in particular, but this guidance so far has generally done little more than re-state the regulations or legislation, though frequently in a more accessible form.

² The Department has issued regulations providing safe harbors for certain financial transactions and relationships pertaining to electronic health records, but the authority to establish such financial safe harbors does extend to the creation of the kind of liability safe harbors discussed in this white paper.

**USING SAFE HARBORS TO REDUCE LEGAL BARRIERS TO IMPLEMENTATION OF
ELECTRONIC HEALTH RECORDS AND HEALTH INFORMATION NETWORKS**

November 2006

A comparable regulatory scheme for health information privacy and security in EHR and HIN environments could issue comparably useful safe harbor regulations and interpretation. For example, in the case of patient notice of HIN participation, an agency could issue regulations (or guidance) describing the form and content of one or more provisions which would provide adequate notice. In the case of EHR authentication, an agency could issue regulations specifying factors which would be considered reasonable and appropriate and therefore in compliance with the law. In neither case would healthcare organizations be required to use the specific provision or authentication factors, but those which chose to do so would be assured their implementation was consistent with the agency's authoritative interpretation of the law.

Developing Content for EHR and HIN Safe Harbors.

An EHR and HIN safe harbors scheme would be adaptable to – and should in fact be based upon – prevailing industry standards and best practices, and would also be transparent and open to the public. Legislation might require implementation of formally-developed industry standards, as HIPAA does for transactions, but that is probably more appropriate for prescriptive legal mandates rather than safe harbors. A better strategy would be to develop proposed safe harbors based on research into healthcare standards and practices, to be finalized after a public comment period open (as is generally required for regulations) to any interested party.

A public safe harbors development process would present a much greater opportunity for public understanding of and input into EHR and HIN policies and practices than current practice. Currently, EHR and HIN policies and practice are developed ad hoc, to some extent in a few standards groups but principally in negotiations among healthcare organizations and vendors. Not only is this activity mostly unknown to the public, for the most part there is not even an opportunity for public understanding and input.

Ad hoc development also leads to avoidable divergence in EHR and HIN policies and practices among organizations. This in itself is a barrier to widespread implementation, since organizations using different policies and practices often find it difficult or even impossible to share networks and information, or find it difficult to adapt to each other when they try. Publicly-developed safe harbors would present common policies and practices all participants could use, again lowering a barrier to implementation.

As noted above, and reflected in HIPAA, there is a valid point that technologies, economic conditions and operating environments are diverse and changeable, often rapidly. However, this point argues for careful execution of a safe harbors strategy, rather than its avoidance. Safe harbors should be carefully chosen and defined to apply to and solve common problems, at a sufficiently general level that they should not need frequent revision. This is also an argument for the inclusion of additional regulatory guidance opportunities, through reports, publications and perhaps opinion letters, so that new developments and distinctive circumstances can be addressed.

**USING SAFE HARBORS TO REDUCE LEGAL BARRIERS TO IMPLEMENTATION OF
ELECTRONIC HEALTH RECORDS AND HEALTH INFORMATION NETWORKS**

November 2006

In practical terms, this process might work for the privacy notices and authentication examples discussed above as follows. Given appropriate enabling legislation, the agency authorized to develop EHR and HIN safe harbors would identify a set of key issues for which uncertainty about legal privacy or security standards appeared to be discouraging EHR or HIN implementation. These issues might very well include privacy notice content and authentication. Initial proposals for their resolution would then be solicited from appropriate stakeholders and interest groups, as well as the public.

Based on this initial feedback, the agency would develop proposed regulations and publish them for comment. The proposed regulations would be sufficiently detailed to permit meaningful comments; for example, the proposed privacy notice regulation might provide one or more provisions which could be adopted, while the proposed authentication regulation might specify that use of two-factor authentication would be considered compliant. Following comments on the proposed regulations, the agency would develop and publish final regulations.

Organizations could choose to implement the policies and practices described in the regulations, and have the agency's assurance they were in compliance; organizations which chose not to do so, would not be penalized per se. For example, an organization could still conclude, based on its HIPAA risk analysis, that two-factor authentication was not a reasonable and appropriate safeguard in its environment. This decision might be open to question in the event of a regulatory investigation or litigation, especially arising from an incident raising the question of the adequacy of authentication, but the mere fact of noncompliance with the safe harbor would not be grounds for a penalty.

Implementation of the Safe Harbor Scheme.

An EHR and HIN safe harbors regulatory scheme would be no silver bullet. Given the complexities of federal and state jurisdiction no agency would be able to cover all the issues. And while ideally, perhaps, EHR and HIN safe harbor regulations should be a federal function, creating significant new federal agency authority can take a long time. Further, achieving a national consensus on appropriate safe harbors is likely to be much harder than achieving it within a state or region. Federal safe harbors are not likely to be available for some time at best.

State-by-state safe harbors, on the other hand, raise the questions of HIPAA applicability and the potential for excessive and unnecessary cross-state variation. While the former question needs more analysis, HIPAA does provide that state laws which are more protective of information control where both HIPAA and state laws apply.

State-based regulations which establish safe harbors more protective than HIPAA should therefore provide assurances of compliance with both state and federal law. Where HIPAA does not provide a clear standard, while state agencies may have limited authority to

**USING SAFE HARBORS TO REDUCE LEGAL BARRIERS TO IMPLEMENTATION OF
ELECTRONIC HEALTH RECORDS AND HEALTH INFORMATION NETWORKS**

November 2006

interpret HIPAA,³ the fact that a state agency has determined that a given policy or practice provides reasonable and appropriate safeguards, following a public comment process, should be very persuasive for HIPAA purposes.

Safe harbors could therefore be implemented using model legislation for state adoption. In order to maximize uniformity, the states implementing such a scheme could establish a coordinating group to keep their safe harbors (and perhaps other health information laws) consistent.

This would not be a complete solution, of course, unless all the states and territories adopted the same scheme and safe harbors, and that is not likely any time soon. Even with a coordinated state-by-state scheme, interstate organizations operating in both states with safe harbors and those without (or those with materially different safe harbors) would face the question whether they could adopt uniform policies and practices across the organization, and comply with both states' laws.

Upon analysis, this problem becomes something of a red herring. Interstate organizations already face the problem of actually or potentially conflicting state requirements, with much less guidance and uniformity than would be possible under a state-by-state safe harbors scheme. Such a scheme would therefore be a clear improvement over the current situation.

The uniformity problem would only arise in the first place for interstate organizations operating in both safe harbor and non-safe harbor states if there was a conflict between the safe harbor of the one state and some legal requirement of the other. One reason such conflicts seem unlikely to arise is that a safe harbors scheme is probably more likely to be adopted by states whose legislators and regulators feel competent in addressing health information technology issues. If legislators and regulators in non-safe harbor states do not feel sufficiently competent in this area to adopt a safe harbors scheme, it seems unlikely they would feel competent enough to implement legal mandates in this area in sufficient depth to create a conflict with other states' safe harbors.

Should this problem arise anyway the nature of safe harbors compliance would allow interstate organizations to resolve it, by adopting policies and practices compliant with the mandate; there would be no penalty for failing to comply with the safe harbor. The same principle would allow resolution of a conflict between different safe harbors provided by different states, should that arise, since an interstate organization could choose between available safe harbors without penalty.

³ Though it is worth noting that the California Department of Managed Care relied heavily on a failure by Kaiser Permanente to comply with the HIPAA security regulations, in imposing a state law penalty for failure to appropriately safeguard protected health information in a publicly-accessible pilot website.

**USING SAFE HARBORS TO REDUCE LEGAL BARRIERS TO IMPLEMENTATION OF
ELECTRONIC HEALTH RECORDS AND HEALTH INFORMATION NETWORKS**

November 2006

A coordinated state-by-state safe harbors approach would therefore allow the incremental development of national uniformity. States which were ready to address EHR and HIN issues could adopt safe harbors reflecting well-accepted, reasonable and appropriate policies and practices; other states could follow their lead when they were ready and if they found such safe harbors acceptable. Healthcare organizations would have an incentive to adopt safe harbor policies and practices to gain some currently available legal certainty, but could move to them as and when it worked for them without penalty.

Conclusion.

As a general rule there are good reasons for governments to tread carefully on technology-related issues, especially in emerging fields like EHR and HIN implementation. However, we seem to have reached a point at which legal uncertainty is itself a barrier to potentially beneficial progress, and governments – as the principal source of the laws – may be especially well-suited for resolving this kind of uncertainty. A carefully managed safe harbors strategy would allow for the reduction of legal uncertainty without imposing prescriptive requirements which would be hard to change if and when they became obsolete. While it would probably be most valuable in the long run for this to be a federal function, in the short run the states could assume a leading role, and reduce legal barriers to EHR and HIN implementation by reducing its attendant legal uncertainty.

Appendix A: Model Electronic Health Records and Health Information Network Safe Harbors Act

The following is a “straw man” model act, intended to stimulate discussion about appropriate methods of implementing a state-by-state safe harbors strategy. It is not intended to be the final version of such legislation, but only to identify key issues and terms.

I. **Short Title.** This Act may be cited as the Model Electronic Health Records and Health Information Network Safe Harbors Act.

II. **Purpose.** The purpose of this Act is to promote the health and safety and protect the privacy of the residents of <STATE>, by facilitating the adoption of electronic health records and health information networks through the development and establishment of uniform or consistent laws, standards, policies and practices providing legal liability-related incentives for the adoption of reasonable and appropriate privacy- and security-related policies and business practices for their operation, management and use.

III. **Definitions.** In this Act:

(1) “Business practice” means a procedure, process or activity used in the operation, management or use of an electronic health record and/or health information network.

(2) “Electronic health record” means an electronic system used to acquire, store, process, retrieve and transmit digital information related to the past, present or future physical or mental health of an individual for the primary purpose of providing health care and health-related services.

(3) “Health information network” means any system for the electronic transmission of digital information between or among electronic health records which are owned, operated and/or used by different entities.

(4) “Personal health information” means any information which (a) identifies or can be used to identify any individual, and (b) pertains to the past, present or future physical or mental health of that individual, the provision of health care to that individual, or the past, present or future payment for the provision of health care to that individual.

(5) “Policy” means written documentation adopted by an organization governing the operation, management or use of electronic health records and/or health information networks, their components, or personal health information.

(6) “Privacy” means an individual’s right to control the acquisition, use or disclosure of personal health information about him- or herself.

**USING SAFE HARBORS TO REDUCE LEGAL BARRIERS TO IMPLEMENTATION OF
ELECTRONIC HEALTH RECORDS AND HEALTH INFORMATION NETWORKS**

November 2006

Appendix A

(7) “Reasonable and appropriate” means consistent with the administrative, financial, and technical capabilities of the organizations to which a safe harbor is intended to apply, when considered in light of the purposes of this Act and the criteria for establishing safe harbors.

(8) “Security” means administrative, physical and technical safeguards used to protect personal health information against unauthorized acquisition, use, or disclosure, and to prevent the unauthorized use or misuse of or harm or damage to electronic health records and/or health information networks.

III. **<ASSIGNED AGENCY> Duties.** The <ASSIGNED AGENCY> shall adopt rules consistent with this Act and in furtherance of its purposes, providing safe harbors for reasonable and appropriate privacy- and security-related policies and business practices for the operation, management and use of electronic health records and health information networks. The <ASSIGNED AGENCY> shall develop such rules as follows:

(1) Not later than <DATE>, and not less than <ANNUALLY> thereafter, the <ASSIGNED AGENCY> shall publish a notice in the <STATE REGULATORY REGISTER> soliciting proposals for safe harbors for electronic health record and health information network operation, management and/or use policies and/or business practices, and for modification of existing safe harbors if applicable. Such proposals shall be received for a period of <SIXTY> days from the date of publication.

(2) After considering the proposals received in response to the notice referred to in subsection III(1) the <ASSIGNED AGENCY>, following consultation with the Attorney General, shall publish proposed safe harbors and/or proposed modifications to safe harbors, as applicable, in the <STATE REGULATORY REGISTER>, subject to a <SIXTY> day comment period.

(3) After considering comments received during the comment period referred to in subsection III(2) the <ASSIGNED AGENCY> shall issue final rules establishing safe harbors and/or modifications to safe harbors as applicable.

IV. **Criteria for Establishing and Modifying Safe Harbors.** In determining whether to establish or modify a safe harbor the <ASSIGNED AGENCY> shall consider the following factors:

(1) The value of the safe harbor in facilitating the adoption and use of electronic health records and health information networks;

**USING SAFE HARBORS TO REDUCE LEGAL BARRIERS TO IMPLEMENTATION OF
ELECTRONIC HEALTH RECORDS AND HEALTH INFORMATION NETWORKS**

November 2006

Appendix A

- (2) The potential implications of the safe harbor for the privacy of <STATE> residents;
- (3) The value of the safe harbor in enhancing the security of personal health information about <STATE> residents;
- (4) Whether the safe harbor may increase the interoperability of electronic health records;
- (5) The costs and burdens of compliance with the safe harbor, including but not limited to policy and business practice change management and the availability and cost of technologies (when applicable);
- (6) Factors affecting adoption of the safe harbor by smaller, rural and safety-net healthcare providers;
- (7) Potential cost-savings to organizations using electronic health records and/or health information networks;
- (8) Whether the safe harbor is consistent with applicable professional, industry and technical standards, guidelines and best practices; and
- (9) Whether the safe harbor is consistent with relevant laws and standards adopted or under consideration by the federal and other state governments, especially but not limited to safe harbors adopted or under consideration by other states pursuant to legislation with comparable intent to this Act.

V. ***Effect of Safe Harbor Compliance.***

- (1) Policies and business practices which are established as safe harbors under this Act shall be considered reasonable and appropriate safeguards for the protection of personal health information.
- (2) The good faith, diligent implementation of any policy and/or business practice established as a safe harbor under this Act shall be a complete defense in any action arising from or pertaining to the acquisition, use, disclosure, alteration or destruction of personal health information, whether the action is for civil or criminal penalties or alleging any violation of an applicable standard of care, to the extent that such action is based upon the operation, management or use of an electronic health record or health information network by the defendant in compliance with such policy and/or business practice.

Appendix B: Electronic Health Records and Health Information Network Safe Harbors Demonstration Rules

The following are sample regulations demonstrating possible regulatory safe harbors. As with the model act, these are not intended to be actual forms of such regulations, but only a demonstration of one way such regulations might be drafted.

<REGULATORY CITATION 1> Regulatory Authority. <CITATION TO ENACTED AND CODIFIED MODEL ELECTRONIC HEALTH RECORDS AND HEALTH INFORMATION NETWORK SAFE HARBORS ACT>

<REGULATORY CITATION 2> Definitions. For purposes of this Rule:

- (1) “Authentication” means a process by which a user’s claimed identity is verified, by presentation of one or more authentication factors.
- (2) “Biometric” means an authentication factor based upon a user’s biological characteristics, such as fingerprints.
- (3) “Factor” means an authentication factor, which may be information (“something the user knows,” such as a password), a biological characteristic (“something the user is”) or a token (“something the user has”). An authentication factor must be presented in order to verify the user’s identity for purposes of access to an electronic system.
- (4) “Notice of Privacy Practices” means any notice published to individual data subjects which is required or permitted by law, which describes uses and disclosures the publishing entity may make of personal health information, and/or individual data subjects’ privacy rights with respect to personal health information about them subject to the control of the publishing entity.
- (5) “Password” means a string of alphanumeric or other characters used as an authentication factor. A “strong” password has at least eight characters, including at least one number.
- (7) “Registration” means a process for verifying the identity of an individual to qualify for user access to personal health information.
- (8) “Token” means an electronic object or device, such as a swipe card, “java bean” or universal serial bus (“USB”) memory stick, which includes information used as an authentication factor when the user possessing the token seeks to access to an electronic system. A “hard” token is a token in which such information has been permanently installed. A “soft” token” is information which is downloaded to a token object or device from another source.

**USING SAFE HARBORS TO REDUCE LEGAL BARRIERS TO IMPLEMENTATION OF
ELECTRONIC HEALTH RECORDS AND HEALTH INFORMATION NETWORKS**

November 2006

Appendix B

(9) “User” means an individual who has been registered and issued a user name and authentication factors for purposes of electronic system access.

<REGULATORY CITATION 3> Exemptions from State Law Penalties and Liabilities.

The following policies and business practices shall be considered reasonable and appropriate, and their diligent, good faith implementation shall be a defense under <STATE> law as provided in <SECTION V(2) OF THE ACT AS CODIFIED>:

<REGULATORY CITATION 3(a)> Notice of Participation in Health Information Network. The following provision, or its material equivalent, may be included in any notice of privacy practices for purposes of disclosing the participation of the organization or individual in a health information network, and/or the implementation of business practices for the acquisition and/or disclosure of personal health information by an organization or individual by use of a health information network, to individuals whose personal health information may be acquired or transmitted through such health information network:^[a]

<ORGANIZATION/INDIVIDUAL NAME> may use a health information network acquire personal health information about you, or to disclose such information to other organizations or individuals.

This health information network is a computerized system for the electronic transmission of personal health information which is used only by healthcare providers, including certain hospitals, physician practices, clinical laboratories and other healthcare professionals and healthcare provider organizations. Your personal health information will only be acquired or disclosed through this network for purposes of healthcare treatment, payment for healthcare, or certain healthcare operational activities. <SPECIFY OTHER PURPOSES CONTEMPLATED, IF ANY>

This means, for example, that we may use the health information network to <EXAMPLE(S) SUCH AS “obtain surgery results from a hospital where you have received such care, for our medical records to help provide you primary care in the future” AND “disclose your current medications to a specialist to support the specialist’s treatment of you”>

You may choose to have us use the health information network to acquire or disclose your personal health information. If you prefer not to have your personal health information acquired or disclosed in this fashion, please

^a This provision is based on the recommendations of the **Connecting for Health Common Framework** (2006), P3: “Notification and Consent When Using a Record Locator Service.”

USING SAFE HARBORS TO REDUCE LEGAL BARRIERS TO IMPLEMENTATION OF
ELECTRONIC HEALTH RECORDS AND HEALTH INFORMATION NETWORKS

November 2006

Appendix B

forward your written request to <APPROPRIATE CONTACT INFORMATION>.

<**REGULATORY CITATION 3(b)**> ***Authentication of Users for Access to Personal Health Information.*** The following policies and business practices may be implemented for the identification and authentication of individuals for purposes of access to personal health information stored in an electronic health record or acquired through a health information network:

- (i) Each user shall be identified by a unique user name.
- (ii) Users shall be authenticated by no fewer than two factors. One factor may be a strong password. The second factor shall be a hard or soft token or biometric.
- (iii) User registration shall be administered by identified individuals authorized in writing to register users by the organization which owns the applicable electronic health record or health information network. Such organizations may delegate operational duties related to identification and authentication, including registration and authorization to register, by written agreement to third parties which are qualified to manage such functions.
- (iv) Users shall be registered upon in-person presentation of a current, governmentally-issued identification credential including a photograph. Written records shall be maintained of each registration.
- (v) Users names, initial passwords and soft tokens may be transmitted to users electronically using encrypted email or other encrypted channels. User names, passwords and tokens may be transmitted to users in-person at the time of registration or by delivery service requiring a signature by the user and return receipt.