



April 26, 2002

Tommy G. Thompson
Secretary, U.S. Department of Health and Human Services
Office for Civil Rights
Attention: Privacy 2
Hubert H. Humphrey Building, Room 425A
200 Independence Avenue, SW
Washington, DC 20201

Re: 45 CFR Parts 160 and 164 (Proposed rule [NPRM] – modification)

Dear Secretary Thompson:

The North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA) is pleased to have the opportunity to submit suggestions for clarification of the proposed modification to the HIPAA privacy rule (NPRM), which was issued on March 27, 2002 in 67 Fed. Reg. 14776-14815. NCHICA is a privately funded, nonprofit organization that actively promotes the advancement and integration of information technology into the healthcare industry. NCHICA has over 250 member organizations nationwide, representing the many sectors of the healthcare industry.

NCHICA has been actively involved in analyzing and providing support to its members regarding the provisions of the final HIPAA privacy rule, entitled "Standards for Privacy of Individually Identifiable Health Information," which was published on December 28, 2000 in 65 Fed Reg 82462-82829. NCHICA's comments on the NPRM below are the result of a collaborative effort among NCHICA's diverse member organizations who, through the activities of established work groups, have developed considerable expertise in the various areas of the privacy rule.

In general, NCHICA believes that the Department of Health and Human Services (HHS) should be praised for the intent behind the proposed modification to the final privacy rule. It is NCHICA's view that these proposed modifications clarify the standards for the protection of the confidentiality of individually identifiable health information without compromising the strong protections afforded to personal health information. Our suggestions for clarification are as follows:

Improving healthcare through information technology and secure communications

3200 Chapel Hill/Nelson Blvd. ● Suite 200 Cape Fear Building ● P.O. Box 13048 ● Research Triangle Park, NC 27709-3048
919-558-9258 (phone) ● 800-241-4486 ● 919-558-2198 (fax) ● www.nchica.org

A. Disclosures for Treatment, Payment & Health Care Operations

Notice of Privacy Practices

(1) We believe that the revisions addressing the use of Protected Health Information (“PHI”) for treatment, payment and health care operations, particularly in eliminating the requirement for a signed consent, are constructive. To the extent that an individual is aware of the privacy policies of a Covered Entity, requiring execution of a consent becomes redundant. In fact, we believe that a primary concern is for individuals to become aware of their rights regarding medical records. Accordingly, providers should be required to put into place policies and procedures to make their Notices of Privacy Practice (“NPPs”) available to all patients and others who are the subject of PHI in any reasonable and reliable manner. The proposed modification requires distribution of NPPs with a receipt of an acknowledgment or documentation that the Covered Entity attempted to obtain such acknowledgment. We find this proposed requirement overly broad, burdensome, and fails to account for the variety of ways patients interact with health care organizations. For instance, many patients may first interact with health care providers or institutions through communication technologies such as the Internet, e-mail, telephone, and other creative means making a single method of acknowledgment impractical for every entity. The larger and more complex the entity, the more likely these concerns will arise.

Hence, rather than requiring an acknowledgment, we suggest that the regulations be revised to require each provider to implement their own policies and procedures specifically adapted to their own operations. The standard should permit each Covered Entity to make available to each relevant individual a copy of its NPP in any reasonable and reliable manner. For example, an entity’s policies and procedures could, in some cases, require a written or electronic acknowledgment, if this is deemed a reasonable and reliable manner for that particular Covered Entity. In other cases, a check-off acknowledgment in the medical record by the provider, subject to audit to demonstrate compliance with the standard, may be acceptable. This is the procedure currently in place for requirements such as “advance directives” and “organ donations.”

We consider such an approach to be advisable for two reasons. First, it is burdensome and difficult to implement the modification as proposed. Second, the requirement for an acknowledgment may hinder providers from further innovation. By requiring written acknowledgment, providers may be deterred from exploring alternative methodologies to show that individuals received notification. For example, the introductory comments to the proposed regulation state, “When electronic notice is provided as part of the first service delivery, the system should be capable of capturing the individual’s acknowledgment of receipt electronically.” This language appears to assume that electronic acknowledgment is sufficient, yet remains inconsistent with the requirement for *written* acknowledgment. Other methodologies to verify receipt may also enter into broad use absent regulations limiting those methodologies to written acknowledgment.

In summary, we recommend that the standard in the final regulation permit the Covered Entity to put into place its own policies and procedures to make available the NPP to patients in any reasonable and reliable manner.

(2) In addition, one goal of the privacy regulations is that individuals should receive an understandable description of the privacy policies of those who retain their medical records. Unfortunately, given the length of the regulations and their complexity, a legally sufficient and readable NPP will likely be numerous pages in length, which could discourage many individuals from actually reading or understanding the Notice. For example, fully describing the use or disclosure of PHI for “healthcare operations” in a readable fashion and with relevant examples could require numerous pages.

Given these concerns, we suggest that the requirements for notice allow a far briefer NPP involving simpler concepts. We therefore recommend that entities be allowed to comply with this

portion of the regulations by supplying notice that could fit on a single page or at least providing a one-page summary with the full notice being available to the patient on request. This notice would do the following: 1) list the entities covered by the notice; 2) inform the individual that the entities listed are subject to internal policies and federal regulations; 3) notify the individual that those policies and regulations protect the privacy of medical records relating to the individual; 4) inform the individual that they have a right, under most circumstances, to obtain copies of their records, to know who has received those records, and to request revisions to those records; and 5) state simply that the entities listed may use and disclose health information relating to the individual for purposes of “payment, treatment, and administrative matters.” (We use the term “administrative matters” rather than “health care operations” as this may be confusing to certain individuals who may assume the term “health care operations” refers to a surgical procedure). While such notice may not contain all the information required under the current regulations, we believe that it would be more likely be read and understood, yet contain the most critical information needed, by the vast majority of individuals.

B. Minimum Necessary and Oral Communications. No comment.

C. Business Associates [§164.532 and Appendix to the Preamble]

NCHICA supports and applauds the Department's proposed extension of the compliance deadline for certain Business Associate agreements and the addition of model Business Associate agreement language. The following are our comments with respect to these changes:

1. Extension. Many of the covered entities that are members of NCHICA have hundreds or even thousands of potential Business Associates. Due to the manner in which the extension is applied, covered entities will be forced to review all of the hundreds or thousands of agreements evidencing their Business Associate arrangements to determine when each agreement is due for renewal and whether the renewal date will fall within the grandfathered time period. Many NCHICA members will not attempt to take advantage of this extension due to the expenditure of time and resources required to make this determination. NCHICA believes that this extension would provide more relief to covered entities if it were applied to all Business Associate agreements, extending the compliance deadline for all Business Associate agreements to April 14, 2004.

In addition, NCHICA notes that the NPRM expressly retains the responsibilities of the covered entities under Sections 164.524, 164.526 and 164.528 commencing on April 14, 2003, even in light of the extension for certain Business Associate agreements. Under these retained sections, covered entities will be required to provide to patients access to their PHI, a right to amend their PHI and the right to an accounting for disclosures of PHI. In many instances, PHI will be maintained in some form by Business Associates of covered entities, and in order to comply with these sections, a Covered Entity will be required to obtain information or require amendments from Business Associates. If, due to the extension, the arrangement agreements relating to particular Business Associates have not been amended to include the Business Associate requirements of the Rule, covered entities will have no mechanism for requiring the performance of their Business Associates under these retained sections. In order to make the extension meaningful to covered entities, the compliance requirements related to these sections should also be extended until April 14, 2004.

2. Model Business Associate Agreement Language. NCHICA believes that the model language for Business Associate agreements provided in the Appendix to the Preamble of the NPRM will be helpful to smaller covered entities that may not have access to form documents or have the funding to engage attorneys to draft agreements on their behalf.

However, NCHICA notes that the model language goes beyond the requirements of the Rule in some instances, two of which are specifically outlined below, and contains requirements that are more onerous than the Rule envisions. Providers may feel compelled to include these provisions in their own Business Associate agreements since they are contained in the model

language.

Please note, NCHICA, through its Business Associate Agreement Work Group, has spent hundreds of hours developing a model Business Associate contract form that could be used by both large and small covered entities as well as Business Associates. This form document represents a consensus of its members inclusive of health plans, payors, large and small hospitals, other health care providers, vendors and suppliers, professional health associations, privacy and security officers, Business Associates, state and local public health departments, and health care attorneys with HIPAA expertise – both in-house and outside counsel. The Work Group recognized that separately-negotiated agreements will be extremely costly in terms of time, legal fees and the management of non-standard agreements that may number in the thousands for larger covered entities. This model form is available freely as a sample document on the NCHICA website [http://www.nchica.org/HIPAA/HIPAA_intro.html]. The form was recently revised to include relevant language from the model Business Associate contract provision of the NPRM.

A. Notice of Privacy Practices. The Rule requires that the contract between a Covered Entity and a Business Associate "[e]stablish the permitted and required uses and disclosures of such information by the Business Associate", and that the contract must provide that the Business Associate will "[n]ot use or further disclose the information other than as permitted or required by the contract or as required by law". With certain exceptions, the contract "may not authorize the Business Associate to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the Covered Entity". Presumably as a method of establishing permitted and prohibited uses and disclosures, the model language contains a requirement that the Covered Entity provide a Notice of Privacy Practices and any subsequent amendments to its Business Associates. This requirement is not contained in the Rule, and would not be necessary to "[e]stablish the permitted and required uses and disclosures of such information by the Business Associate". The particular uses and disclosures permitted for Business Associates would be necessarily contained in either the Business Associate agreement itself or in the underlying arrangement agreement. A requirement to provide the Notice of Privacy Practices to each Business Associate of a Covered Entity will be extremely burdensome, particularly with respect to provision of subsequent amendments to the Notice of Privacy Practices. Because this is not required by the Rule, this section should be removed from the model language.

B. Termination. In the section entitled "Termination for Cause," the model language makes it mandatory that the agreement be terminated if a breach by the Business Associate is not cured or a violation ended. Section 164.504(e)(1)(ii) of the Rule provides that, in order for the Covered Entity to remain in compliance with the Rule, if the Covered Entity discovers a material breach or violation of the Business Associate under its agreement, if the breach cannot be cured or the violation ended, the Covered Entity must have terminated the agreement "if feasible; or (B) [i]f termination is not feasible, reported the problem to the Secretary." Section 164.504(e)(2)(iii) requires that a Business Associate agreement "[a]uthorize termination of the contract by the Covered Entity, if the Covered Entity determines that the Business Associate has violated a material term of the contract", but does not make such termination mandatory. The preamble to the final rule recognizes termination, although expected by HHS, is not mandatory. See 65 Fed. Reg. 82505 (Dec. 28, 2000).¹ We, thus, recommend that the model agreement reflect the final rule by making the following revision:

¹ "The rule now stipulates, however, that if the Covered Entity is unable to cure a material breach of the Business Associate's obligation under the contract, it is expected to terminate the contract, when feasible. This qualification has been added to accommodate circumstances where terminating the contract would be unreasonably burdensome on the Covered Entity, such as when there are no viable alternatives to continuing a contract with that particular Business Associate. It does not mean, for instance, that the Covered Entity can choose to continue the contract with a non-compliant Business

In the first sentence of section (b) of “Obligations of the Covered Entity” replace the phrase “and terminate this Agreement” with “and, if feasible for the Covered Entity, terminate this Agreement.”

C. Access to Records. We suggest that the provisions in the model language relating to the Business Associate’s duty to make available to the Secretary its internal practices, books, and records relating to the use and disclosure of PHI be clarified to specify that the Business Associate’s duty in this regard is limited to the disclosure of (i) its policies and procedures relating to uses and disclosures and (ii) the records of such uses and disclosures, and does not include the disclosure of the underlying data. For some Business Associates, such as attorneys, the underlying data may contain embedded work product that is privileged or confidential.

D. Uses and Disclosures Related to Marketing

Comment – marketing information communicated at patient's request:

We recognize that a health care provider may forward marketing information to a patient from time to time because the patient has asked the provider to keep them informed about such information without signing a HIPAA-compliant authorization. For example, a patient may send a letter to his physician asking for information about a particular drug or treatment, although there is no current treatment being received by the patient. Another example would be when a patient who, during an appointment with their physician, expresses concern about the care of their child or parent and then requests the physician to forward information about items or services to their minor child or parent. In such a case, the patient would have had to execute formal HIPAA authorizations to receive this requested information. As a practical matter, physicians may forget to obtain that authorization or it may be impractical to get that formal authorization. The physician who then forwards the requested marketing information, absent a formal authorization, may subject themselves to sanction under the privacy rule.

Thus, we suggest that the definition of marketing be amended to add at its end the following exception:

“or
(4) in response to a request by a patient of a health care provider.”

Comment – telephonic or instant messaging communications:

The exception to face-to-face communications does not recognize that individuals may communicate directly and contemporaneously with their health care provider via telephone or electronic means, e.g., via the Internet. This especially may be the case for shut-ins and persons living in rural areas. Such communication may be identical to a face-to-face communication. We also recognize the potential for abuse of such communications where, during the course of a telephonic or instant messaging conversation, the Covered Entity attaches pre-recorded marketing information to the communication or uses electronic or other means to contact numerous people at once.

We suggest the following additional exception be added to 45 CFR 508(a)(3)(i):

“(C) A telephonic or electronic communication held exclusively between a health care provider and a single individual that is held contemporaneously between the parties and where no part of the communication from the Covered Entity is prerecorded.”

Associate merely because it is more convenient or less costly than contracts with other potential Business Associates.” 65 Fed. Reg. 82505 (December 28, 2000).

E. Parents as Representatives of Unemancipated Minors

NCHICA agrees with the clarification described in the NPRM.

F. Uses and Disclosures Related to Research

164.508 Uses and disclosures for which an authorization is required

With regard to research, the proposed modifications would: (1) establish a single set of required elements for all authorizations; (2) eliminate the distinction between research that includes treatment of the individual and research that does not, and the previous requirement of additional elements in an authorization for research that includes treatment; (3) allow researchers to use a single form that may contain the authorization for use/disclosure of PHI in combination with the informed consent to participate in the research or any other legal permission; and (4) specify that the expiration date of the authorization or event may be “end of the research study” or “none” if the authorization allows disclosure of identifiable health information to a research database or repository. NCHICA supports these proposed modifications, which will lessen the potential for confusion among research participants and significantly reduce administrative burdens on researchers.

164.532 Transition provisions

Changes proposed by the NPRM to this section would: (1) permit use/disclosure for research of PHI created either before or after the rule’s compliance date if an authorization or other legal permission was obtained from the individual before the compliance date; and (2) grandfather in the use of PHI created in research for which the individual signed an informed consent to participate in the study or if an Institutional Review Board (“IRB”) waived the consent requirement for that study. Again, NCHICA agrees that there is a need for establishing a single, consistent set of transition provisions related to research. However, we suggest that, for individuals joining an ongoing research study, HHS clarify that any authorization forms approved by an IRB in existence by the date of compliance with the final rule would be grandfathered so that it would not be necessary to amend the authorization to include required privacy language until the next annual review by an IRB, not to exceed more than 12 months following the enforcement date.

164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required

At 164.512(i)(2)(ii) the NPRM proposes to revise the waiver criteria under which an IRB or Privacy Board may waive the requirement for individual authorization relating to the use or disclosure of PHI for research purposes based on specific criteria. As proposed, these waiver criteria will be consistent with existing Common Rule criteria related to risk, and ensure that identifiers are protected against improper use or disclosure and/or destroyed at the earliest possible time, unless there is a research or health justification for retaining the identifiers or such retention is otherwise required by law. We agree with the clarification in the proposed modification that an “IRB or Privacy Board waiver of authorization... [may] encompass a partial waiver of authorization for the purposes of allowing a researcher to obtain protected health information necessary to recruit potential research participants. For example, even if an IRB does not waive informed consent and individual authorization for the study itself, it may waive such authorization to permit the disclosure of protected health information to a researcher as necessary for the researcher to be able to contact and recruit individuals as potential research subjects.”

G. Authorization No comment other than as above.

H. De-identification

164.514. Other requirements relating to uses and disclosure of protected health information.

Throughout the privacy rule and the NPRM, HHS states that it is encouraging de-identification as an effective method for protecting privacy. The current rule allows two methods of de-identification: (1) a statistician method, and (2) a "safe harbor" that requires the removal of all of 18 identifiers of the individual or of relatives, employers, or household members of the individual. The Department has received little feedback regarding the statistician methodology but is aware of a general view among covered entities that "the statistical method is beyond their capabilities."

In the final rule, HHS referenced two government reports (e.g., Statistical Working Paper 22) that describe techniques that are considered when statistical professionals consider the risk of re-identification in regard to the release of large "de-identified" data compendiums, such as analyses of Census or IRS information. Techniques utilized for reducing the risk of re-identification include: removing direct identifiers; reducing the number of variables on which a match might be made; and limiting the distribution of [such de-identified] records through a "data use agreement" or "restricted access agreement" in which the recipient agrees to limits on who, among the recipient's workforce, for instance, can use or receive the data. There have been many complaints that the "safe harbor" method would produce data unsuitable for research and a variety of other uses. This is not surprising, since the "safe harbor" was not designed for research, but to be a reasonably safe method under which an individual with absolutely no knowledge of de-identification could 'sanitize' their records and literally publish them on the Internet if they wished. Apparently, due to the perceived lack of enthusiasm for the "statistical" method in the NPRM, the Department "requests comment on an alternative approach that would permit uses and disclosures of a limited data set which does not include facially identifiable information but in which certain identifiers would remain."

NCHICA is supportive of the addition of an alternative approach in the final privacy rule, and includes some additional suggestions below:

With this alternative approach, "direct identifiers" (i.e., name, street address, telephone and fax numbers, e-mail address, social security number, certificate / license number, vehicle identifiers and serial numbers, URLs and IP addresses, full face photos and comparable images) would be removed. However, retention of the following identifiable information would be permitted: admission, discharge and service dates; date of death; age (including over age 90); and five-digit zip code.

The Department solicits further comment on whether a geographic code such as city, county, precinct, etc. would be needed in addition to, or be preferable to, five-digit zip. NCHICA proposes that the alternative approach permit, in addition to a five-digit zip, an additional geographic code. Further, NCHICA proposes that, because many preexisting databases include date of birth (DOB), this should be permitted in the limited data set.

Disclosure of the limited data set by a Covered Entity would require the Covered Entity to obtain from the recipient(s) a "data use or similar agreement, in which the recipient would agree to limit the use of the limited data set to the specified purposes in the privacy rule", limit who can use or receive the data, and agree not to re-identify the data or contact the individuals.

The Department states that the limited data set could not be used for "general purposes" but

only for "research, public health, and health care operations purposes."

NCHICA agrees that the alternative approach, incorporating a data use or a similar agreement, prohibiting re-identification, and not allowing any attempt to contact the individual would provide appropriate and reasonable alternative means of de-identification under the rule. Accordingly, with these adequate safeguards, there should be no reason to limit the use of the 'limited data set' only to research, public health and very circumscribed health care operations. Further, data that is de-identified and restricted by the Covered Entity in its data use agreement should no longer be subject to particular uses or limitations by HHS as it would be 'outside the rule' in a similar manner as "safe harbor" data.

I. Technical Corrections/Clarifications - No comment.

- i) No comment.
- ii) No comment.
- iii) No comment.
- iv) No comment.
- v) No comment.
- vi) No comment.
- vii) No comment.

J. Implementation Issues - No comment.

K. Miscellaneous/Other Comments related to the Privacy Rule - No comment.

NCHICA appreciates the opportunity to comment on the NPRM and thanks HHS for serious consideration of its suggested clarifications to the proposed modifications to the privacy rule.

Sincerely,

W. Holt Anderson
Executive Director