June 1, 2009

Federal Trade Commission
Office of the Secretary
Room H-135 (Annex M)
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Attention: Health Breach Notification Rulemaking, Project No. R911002

The Minnesota e-Health Initiative in conjunction with the members of the Minnesota Privacy and Security Workgroup are pleased to submit comments on the proposed Federal Trade Commission's (FTC) breach notification requirements, notice of proposed rulemaking and request for public comment. We appreciate the effort of the FTC to seek public comment on the proposed rules requiring vendors of personal health records and related entities to notify individuals when the security of their individually identifiable health information is breached.

We generally support the proposed rule but offer feedback and recommendations to improve the rule, specifically we urge the FTC to:

- Include the terms "accessed" and "disclosed" as a part of the definition and rationale for the term "acquired"
- Further develop criteria for, or define, the security measures that organizations need to have in place to not trigger breach notifications for "reasonably should have been known"
- Change the requirement to post breaches' on organizations websites from 6 months to 30 days
- Have a submission of breach logs from organizations be on a set schedule by region

Our detailed comments and recommendations on specific components of the proposed rule are attached.

Should you have questions you may contact:

Michael Hawton, Project Manager
Minnesota Privacy and Security Program
Minnesota Department of Health
PO Box 64882, St. Paul, MN 55164-0882
Phone: (651) 201-3598
Email: michael.hawton@state.mn.us

Sincerely,

Scott Leitz
Assistant Commissioner
Minnesota Department of Health

About the Minnesota e-Health Initiative and Minnesota Privacy and Security Program

This coordinated response to the notice of proposed rulemaking and request for public comment was created by inviting and engaging multiple stakeholders from within the Minnesota healthcare system that participate in the Minnesota e-Health Initiative and the Privacy and Security Workgroup.

The Minnesota e-Health Initiative is a public-private collaborative in Minnesota whose vision is to accelerate the adoption and use of health information technology in order to improve health care quality, increase patient safety, reduce health care costs and improve public health. The Minnesota e-Health Initiative is guided by a statewide Advisory Committee with 25 representatives from interested and affected stakeholders. Details on the Minnesota e-Health Advisory Committee can be found at: http://www.health.state.mn.us/e-health/advcommittee/index.html.

The privacy and security workgroup as a part of the Minnesota e-Health Initiative represents a broad spectrum of stakeholders and representatives from over 25 health care organizations across the state. The workgroup is chaired by Laurie Beyer-Kropuenske of the Minnesota Department of Administration and coordinated by the Minnesota Privacy and Security Program (MPSP). Details on the initiative can be found at: http://www.health.state.mn.us/ehealth/.

The MPSP works to develop and implement strategies and projects that support and meet an essential purpose of the Minnesota e-Health Initiative of enhancing infrastructure through "policies for strong privacy and security protection of health information". Details on MPSP can be found at: http://www.health.state.mn.us/e-health/privacy/index.html.

T he Minnesota e-Health Initiative and Minnesota Privacy and Security Workgroup Comments and Recommendations on the Federal Trade Commission's proposed Health Breach Notification Rulemaking, Project No. R911002

General Comments –
The comments in this section are general in nature and are not in response to specific questions or topics identified in the notice of proposed rulemaking and request for public comment.

- We strongly support the recommendation to use the NIST standards for encrypting and destroying data as outlined in the U.S. Department of Health and Human Services guidance on technologies and methodologies to render personal health information unusable, unreadable and indecipherable to unauthorized individuals.

Comments on Specific Items Identified in the Notice of Proposed Rulemaking –
Proposed section 318.2: Definitions
Comments specific to this proposed section:

- The rule proposes a definition of "acquisition" that is separate from the terms "accessed" and "disclosed"; by parsing these terms out and relying on the definition of "acquisition" as the criteria that initiates notification, the requirement on vendors of personal health records (PHRs) for breach notification becomes much more narrow. We would recommend that for both the HHS security guidance and FTC breach notification rule that a consistent definition of breach be used that is inclusive of all of the following terms: "acquired", "accessed", or "disclosed."
  The proposed rule adds a sentence to the definition of breach of security and exclusively uses the term "acquisition". We would recommend that the proposed sentence read, "Unauthorized access, acquisition, or disclosure will be presumed for unsecured PHR identifiable health information unless the vendor of personal health records, PHR related entity, or third party service provider that experienced the breach has reliable evidence showing that there has not been, or could not reasonably have been, any unauthorized access, acquisition, or disclosure of such information."

Additional instances (examples) where, even though the standard for de-identification under 45 CFR 164.514(b) is not met; there is no reasonable basis to believe that information is individually identifiable

- Currently under 45 CFR, the Limited Data Set (LDS) is considered to be a reasonable and accepted method for securing personal health information (PHI). Since there is no way to eliminate the risk of re-identification of PHI entirely, covered entities should not be held accountable for the actions of individuals who attempt to re-identify PHI. The accountability for covered entities and business associates is in ensuring the requirements for securing and protecting PHI are met. With this context in mind, we recommend the following:
  - The LDS needs to be considered an instance where there is no reasonable basis to believe that information is individually identifiable.
  - The LDS should always be considered compliant with security requirements if it is stripped of direct identifiers.

Proposed section 318.3: Breach notification requirement
Comments specific to this proposed section:

- We would like to recommend that the FTC or HHS develop criteria for or clearly define "reasonably should have been known." Without criteria or clear definition, an organization's interpretation of this phrase may be constantly challenged if:
    - An organization's instituted security measures do not clearly align with the government's understanding of what constitutes reasonable security measures; or
    - The ambiguity caused by a lack of a definition or criteria has organizations being required to complete unnecessary breach notifications.

  The criteria or definition should identify at least what constitutes "reasonable security measures" including identifying what constitutes "breach detection measures" so that organizations can understand when HHS and/or FTC may determine an organization should have "reasonably known" of a breach.

Proposed section 318.4: Timeliness of notification

Comments specific to this proposed section:

- Any organization that collects or manages PHI should be open about PHI privacy and security policies and best practices. This includes informing individuals about incidents such as breaches of unencrypted PHI that may have been accessed, acquired, or disclosed by unauthorized persons. One purpose of notifying individuals of such incidents is to enable these patients to take action that will protect themselves against, or mitigate the damage from, identity theft or other possible harm.

  For this reason, it is important to notify affected individuals in the most "***expedient time***" possible after the discovery of an incident involving unauthorized access to notice-triggering information.

  The proposed rule indicates that the timing for a notice is, "in the most expedient time possible and without unreasonable delay."

  To ensure that timely and helpful notice to affected individuals is provided, we recommend the following best practices:
    - First, conduct a preliminary internal assessment of the scope of the breach and then plan for and institute your organization's plan to contain and control the systems affected by the breach.
    - Second, after an organization determines what, if any, unsecured PHI was accessed, acquired, or disclosed by an unauthorized person, the notification to affected individuals should be completed in ten days from the date of the determination of the breach.

  In addition a reasonable amount of time may be allowed to complete the notification for the following reasons:
    - Legitimate needs of law enforcement if notification would impede a criminal investigation.
    - Taking necessary steps to determine the scope of the breach and restore reasonable integrity to the system(s) prior to notification.

Proposed section 318.5: Methods of notice

Comments specific to this proposed section:

- There is a substantial concern about the requirement to send first class mail breach notification to the individual or next of kin of the individual, if the individual is deceased. The inclusion of the next of kin notification is in conflict with our state laws on access to medical information. Proper validation of the "next of kin" and a process to accomplish this validation would need to be developed. Potentially, to notify a family member of a breach, would disregard the privacy of the medical information of the deceased party. In Minnesota, the health information of deceased individuals is protected. A requirement to send this information to a deceased persons "next of kin" would have us releasing protected health information to a potentially unknown party. In addition, such notification is not necessary to a "next of kin" if it is determined that more harm is likely to result from the notification than from an inappropriate dissemination of PHI of unknown consequence. A case in point: an agency that treats individuals for sexual offenses; may in some instances, determine that severe harm could result to a family from the disclosure of former treatment and would not notify the family regarding a potential breach.

  Our preferred recommendation is to have the language regarding "next of kin" removed from the guidance. As an alternative, we would like to recommend a statement in the guidance that reads something similar to, "covered entities and business associates shall attempt to notify the next of kin, provided they are readily identifiable and their identity is verifiable, and the notification to next of kin is allowed for in state law."

- It is our belief that posting breaches to an organization's website for 6 months is onerous. We recommend that the duration for posting breaches on websites be 30 days. In addition, we would recommend that an "official or legal notice" in the local print media be the preferred method for media notification.

- The proposed breach notification requirements indicate that organizations must log every breach, including those breaches of unsecured PHI that involve less than 500 patients, and to report breaches on an annual basis beginning from the date of the first breach. We have two concerns with this requirement as currently drafted:
  - We are concerned with the need to submit a log of every breach of unsecured PHI for less than 500 patients to the government on an annual basis. Organizations may potentially have numerous breaches that involve 1-10 patients. Reporting on these breaches that are smaller in scope creates a significant administrative burden for both providers and the government. We would recommend that a provider be required to log and report breaches to the government only when a breach notification threshold for unsecured PHI of 50 patients is reached or exceeded.

  - Our second concern relates to the requirement that reporting of breaches begins 12 months from the date of the first breach. Understanding that the government may not want all breach logs to come in on the same day of the year, we recommend that breach logs be submitted annually, by region, on a specific date. This recommendation will simplify the process of reporting breaches because organizations can more systematically prepare and schedule the required logging and reporting.