



October 23, 2009

Submitted via the Federal eRulemaking Portal: <http://www.regulations.gov>

U.S. Department of Health and Human Services
Attention: HITECH Breach Notification
Hubert H. Humphrey Building
Room 509F
200 Independence Avenue, SW
Washington, DC 20201

Re: Interim Final Regulations for Data Breaches

Dear Sir or Madam:

Molina Healthcare, Inc. is writing to offer comments in response to the interim final regulations and revised security guidance that were issued in the *Federal Register* on August 24, 2009 pursuant to the Health Information Technology for Economic and Clinical Health (HITECH) Act. (74 Fed. Reg. 42740).

Molina Healthcare is a multi-state health care organization that arranges for the delivery of health care services to persons eligible for Medicaid, Medicare, and other government-sponsored programs for financially vulnerable individuals. Molina Healthcare's subsidiaries in California, Florida, Michigan, Missouri, Nevada, New Mexico, Ohio, Texas, Utah, and Washington currently serve over 1.4 million low-income members.

Molina Healthcare, Inc. is committed to advancing an interoperable system in which health information can be shared electronically in a secure and efficient manner. We are committed to satisfying every state and federal law protecting the privacy of the personal and health information of our members and patients. Therefore, we support federal efforts to protect the privacy and security of protected health information (PHI).

After reviewing the interim final regulations proposed by your agency, we are writing to express our support for the regulatory provisions and the guidance. Specifically, we want to express our strong support for the threshold harm standard. Without a harm threshold, such breach notifications may lead to increased costs and administrative burden on providers and plans, including government health programs, such as Medicare and Medicaid.

We believe the harm threshold is a critical element in deciding whether an impermissible use or disclosure of PHI constitutes a breach and whether any risk of harm to an individual exists. A threshold harm standard is vital for effectively identifying affected individuals and alerting them when a data breach occurs. Incorporating such a standard into federal regulations helps ensure that HIPAA covered entities properly notify affected individuals without unnecessarily alarming consumers where no significant risk of harm exists thereby possibly diluting the importance of a notification that might come to an individual in a circumstance where a risk of harm actually exists. We agree with HHS' assessment that such a standard aligns with existing state requirements and federal agency guidance.

In addition to the threshold harm standard, we believe the following provisions are significant in order to allow HIPAA covered entities and business associates to successfully implement the HITECH provisions:

- **Security Guidance.** Molina Healthcare supports the updated security guidance issued by HHS as a voluntary standard; it gives HIPAA covered entities and their business associates the option of using the specified technologies and methodologies to create a "safe harbor" from data breaches. The voluntary guidance will be helpful for HIPAA covered entities and business associates of various sizes and with diverse needs, resources, and systems based on their business operations.
- **Definition of a Breach.** The regulations define a breach as the acquisition, access, use, or disclosure of PHI in a manner not permitted by the regulations which compromises the security or privacy of the PHI. The regulatory definition of breach helps clarify when the security or privacy of PHI is considered compromised and when a significant risk of financial, reputational, or other harm to an individual exists. The evaluation factors and the practical examples included in the preamble will substantially help HIPAA covered entities and their business associates assess whether a breach has, in fact, occurred and be aware of HHS' expectations for how to interpret and implement the HITECH requirements.
- **Notices to Individuals.** Molina Healthcare is committed to notifying affected individuals in the event that a data breach occurs. We stand ready to work with your agency in developing models or other notices that can be used by HIPAA covered entities to ensure that individuals receive written information in plain language that is easy to understand and that adequately informs consumers about how to protect themselves if a breach has occurred.
- **Enforcement Delay.** We appreciate the discussion in the preamble which explains the ambiguity between the date in the HITECH statute regarding when the breach notification requirements will take effect and the date when HHS has authority to take enforcement action based on violations. While we appreciate that your agency will use discretion to not impose sanctions for entities failing to provide the required

notifications prior to February 22, 2010, we remain committed to working in good faith to implement the HITECH requirements.

Issues That Merit Additional Guidance

Molina Healthcare has also identified two issues that we believe would benefit from additional guidance or clarifications from your agency.

Annual Reporting of Breaches Affecting Less Than 500 Individuals

Issue 1: HHS should change its reporting requirements for HIPAA covered entities to report breaches affecting less than 500 individuals.

Discussion 1: The HITECH Act, section 13402(e)(3) provides that if a breach occurred that affected less than 500 individuals, then “the covered entity may maintain a log of any such breach occurring and annually submit such a log to the Secretary documenting such breaches occurring during the year involved.” HITECH §13402(i) sets out that HHS shall subsequently report to Congress the number and nature of such breaches and the actions taken in response.

We appreciate the ability of covered entities to maintain a log of breaches affecting less than 500 individuals and to annually report this information to HHS within 60 days following the end of a calendar year, as allowed by 45 C.F.R. §164.408(c). We believe such processes will foster consistent and streamlined reporting for HIPAA covered entities in these situations.

On or around October 2, 2009, HHS released Instructions for HIPAA covered entities to annually report data breaches involving less than 500 individuals which directed covered entities to electronically submit a separate breach reporting form for each incident to fulfill the requirement for reporting to HHS. While we recognize that the regulation requires covered entities to provide the notification in the manner specified on the HHS website, we are concerned that in practice the recently-issued Instructions will have the unintended consequence of negating the ability of HIPAA covered entities to maintain a log and submit it to HHS as set forth in the statute.

We recognize that HHS will need a standard reporting process that enables the agency to make its required reporting to Congress. Molina Healthcare supports efficiency and standardization of reporting processes to enable HHS to aggregate data from diverse HIPAA

covered entities. We stand ready to provide additional support and information to assist HHS with achieving these results.

Recommendation 1: To better align HHS' reporting expectations with the HITECH statutory provisions, we respectfully request that HHS change its process and related Instructions which currently require covered entities to complete and submit to HHS a separate report form for each breach involving less than 500 individuals. As an alternative approach, we recommend that HHS allow covered entities to maintain an electronic log that tracks breaches affecting less than 500 individuals that contains the information necessary to enable HHS to make reports to Congress as required by the HITECH Act. The electronic log could include the categories of information currently being solicited on the reporting form.

Secure and Accurate Reporting of Data Breaches

Issue 2: The current process for HIPAA covered entities to report data breaches to HHS should specify how HHS will ensure the privacy, security, accuracy, and integrity of the process for efficient and effective data breach reporting.

Discussion 2: Since HIPAA was enacted and the privacy and security rules were promulgated, covered entities have become accustomed to ensuring the privacy and security of their customers' data in their business operations. Many of these same business processes and methodologies serve the dual purpose of protecting individuals' health data as well as organizations' confidential proprietary data.

In reviewing the interim final regulations and the related Instructions for covered entities to report data breaches to HHS, we are concerned that the current reporting process allows data breach reports to be submitted without fulfilling sufficient expectations for ensuring the privacy, security, accuracy, and integrity of the data being reported. For example, the current process lacks an authentication methodology that could be implemented as a prerequisite to a person or entity submitting a breach report. Without such a process, it is reasonably foreseeable that imposters or hoaxers could name any organization and submit false breach reports to HHS. In addition, without any verification process from HHS after a report is received (e.g., HHS sending an email to a company's privacy officer stating that a breach report was received), there is little opportunity for covered entities to become aware of such a situation if it were to occur.

Page 5

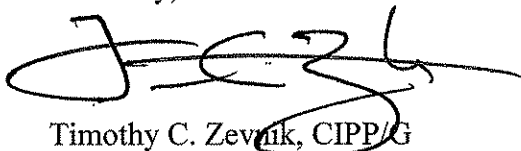
U.S. Department of Health and Human Services
Attention: HITECH Breach Notification

Building on our experiences with implementing the HIPAA privacy and security protections, we believe that HHS should consider implementing technologies and methodologies that enable the agency to more effectively receive electronic data breach reports through a private, secure process that ensures the accuracy and integrity of the information being received. For example, HHS should consider using an electronically secure process for individuals and entities to submit data breach reports, such as email or an Internet process that uses encryption or a process that requires a log-in and a password to gain access to a secure website. HHS should also implement technologies and methodologies that enable the agency to verify the identity of reporters, ensure that reported information is accurate before the data are made publicly available or reported to Congress, while ensuring that the information being solicited from HIPAA covered entities is sufficient for HHS to fulfill its enumerated responsibilities under the HITECH statute.

Recommendation 2: We recommend that HHS implement a process for HIPAA covered entities to submit beach reports that contains several elements: (1) the process should be electronic and require written reports to be submitted; (2) authentication of an individual or organization should occur at the time a data breach report is being submitted electronically to HHS; (3) verification should be provided to an individual or entity submitting a data breach report by providing written notice that a data breach report was, in fact, received by HHS; (4) the privacy and security of information being reported electronically to HHS should be done through a secured website, encryption processes, or similar methods; and (5) the process should employ technologies or methodologies and explain how HHS will validate and ensure the accuracy of reported data before information is made available to the public and reports are made to Congress.

We appreciate the opportunity to provide comments on this important topic.

Sincerely,



Timothy C. Zevnik, CIPP/G