Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) provided the U.S. Department of Health and Human Services (HHS) with the authority to craft privacy protections by regulation when the U.S. Congress failed to pass comprehensive health privacy legislation by its self-imposed deadline of August 21, 1999. Following the principles and policies laid out in the recommendations for national health information privacy legislation HHS submitted to Congress in 1997, HHS drafted regulations to guarantee patients new rights and protections against the misuse or disclosure of their health records. Following an extensive comment period, the final rule -- "Standards for Privacy of Individually Identifiable Health Information" (the privacy rule) -- was released December 20, 2000.

The privacy rule took effect on April 14, 2001. Among other things, it creates national standards to protect individuals' personal health information and gives patients increased access to their medical records. As required by HIPAA, the privacy rule covers health plans, health care clearinghouses, and those health care providers who conduct certain financial and administrative transactions electronically. Most covered entities must comply with the privacy rule by April 14, 2003; small health plans have until April 14, 2004.

A key element of the privacy rule is the requirement that covered entities put in place safeguards to ensure the security of individually identifiable health information (called protected health information or PHI in the privacy rule). The regulation establishes the privacy safeguard standards that covered entities must meet, but it leaves detailed policies and procedures for meeting these standards to the discretion of each covered entity. In this way, the rule allows the implementation of the standards to be flexible and scalable, so as to account for the nature of each entity's business, and its size and resources.

As set out in the rule, covered entities must adopt written privacy procedures. These must include who has access to protected information, how it will be used within the entity, and when the information would or would not be disclosed to others. Covered entities must also takes steps to ensure that their business associates protect the privacy of health information.

Business Associates

In using the regulatory authority provided to it by HIPAA, HHS established the concept of a "business associate" so as to extend privacy protection beyond the limited jurisdiction conferred by HIPAA. Under the statute, HHS has the authority to regulate those who create and disclose health information, but not the many key stakeholders who receive that health information from a covered entity. Although HHS indicated in the commentary accompanying the rule that a statutory approach would have been preferable, they asserted that the issue of privacy was too important to justify their abandoning an attempt to extend privacy protection beyond HIPAA jurisdictional boundaries.

HHS therefore uses its authority over covered entities to regulate the flow of information from covered entities to non-covered entities. The privacy rule requires that a covered entity limit the disclosure of PHI to business associates only after the covered entity has

obtained specified satisfactory assurances from the business associate that it will appropriately handle the information.

Business Associate "Assurances"

The privacy rule requires that the satisfactory assurances obtained from the business associate be in the form of a written contract (or other written arrangement) between the covered entity and the business associate, and that these contain the specified elements set out in the rule.

In modifications to the privacy rule released August 14, 2002, HHS provided model business associate provisions in response to numerous requests for guidance. In the accompanying commentary, HHS indicated that they intended the sample provisions to help covered entities more easily comply with the business associate requirements of the privacy rule. HHS noted that use of the model provisions is not required for compliance with the privacy rule.

The sample provisions are designed to be adapted to the business arrangement between the covered entity and the business associate and to be incorporated into a contract drafted by the parties; the provisions are not intended to serve as a complete contract.

HHS Call for Public/Private Collaboration

In recognition of the magnitude of the implementation effort required by the privacy rule, HHS stated in the commentary accompanying the rule of their willingness to work with trade and professional associations to develop guidance and provide technical assistance so that they can help their members understand and comply with the new standards. The sample provisions are tangible evidence of HHS' acting on this commitment.

HHS further indicated that for the implementation efforts to be successful, the various public and private participants inside and outside of the U.S. health care system would need to work together to assure that their competing interests remain in balance so that an ethic that recognizes and respects the importance of privacy is established. They indicated that, in developing the final regulations, simplifying the administrative burden was a significant consideration. HHS states that the final privacy rule is designed to encourage the development of significant standardization through the efforts of professional associations and others, with the objective that this will reduce costs and facilitate greater consistency across providers and other covered entities.

NEMA Sample Business Associate Language

NEMA members often require access to or receive from their customers PHI in order to maintain their existing medical equipment, to develop new medical equipment, or to provide associated related services. NEMA members have a strong interest both in protecting patient privacy and assisting their customers in meeting their privacy requirements in their dealings with NEMA members. Because NEMA members may be business associates under the privacy rule, and members' customers may be covered entities and therefore needing to have business associated arrangements in place between the parties, NEMA deemed it appropriate that it undertake the development of standard business associate provisions for use by its membership.

NEMA feels that this action is consistent with HHS' call for trade associations to take such steps. The sample language NEMA has developed allows a member to use its

standard sales and service terms and conditions, and by adding the NEMA provisions, satisfy the business association assurances requirement of the privacy rule. Members' use of the NEMA sample language and its close adherence to the spirit and letter of the required language aligns NEMA and its members to HHS' objective for increased administrative efficiencies through enhanced consistency and standardization within the U.S. health care system.

NEMA Outreach Activities

NEMA as an organization was founded with similar objectives, and its history provides ample evidence that real gains are possible through industry-wide adherence to national standards. Many customers of NEMA members are members of trade associations themselves. As encouraged by HHS, NEMA is now reaching out to these associations to make them aware of the NEMA sample business associate provisions with the hopes that these associations will raise awareness within their own membership.

NEMA sees little benefit if each covered entity negotiates unique business associate provisions with its business associates. But we see serious downside impacts because of the large number of business interrelationships in the U.S. health care system. NEMA and its members believe that a major administrative overhead can be avoided if all parties align closely to the sample language HHS has offered.