MEMO

To: Interested Parties

From: Jim Pyles

In reviewing the recently issued HIPAA Security regulations, there appears to be a serious privacy problem which even HHS acknowledges. 68 Fed. Reg. at 8,333 (February 20, 2003). The final Security Regulations are "effective" on April 21, 2003 (one week after the final compliance date of the amended Privacy Rule), but covered entities do not have to comply with the new security standards until two to three years later. The Security Standards compliance date for most covered entities is April 21, 2005 and April 21, 2006 for small health plans. 68 Fed. Reg. at 8,334.

Accordingly, covered entities will have "regulatory permission" to use and disclose identifiable health information (under the amended Privacy Rule) for two to three years before they have to adopt basic security measures to protect the privacy of the information. (Keep in mind that the regulations implementing the enforcement portions of HIPAA have not even been issued in proposed form. See 68 Fed. Reg. at 8363).

HHS' views about the importance of the Security Standards for the protection of medical privacy are instructive. HHS notes that covered entities "must assure their customers" that the confidentiality of their identifiable health information will be protected. 68 Fed. Reg. at 8334. The confidentiality of health information is threatened by the "risk of improper access to stored information" and as well as by the "risk of interception during electronic transmission". HHS notes that "currently, no standard measures exist in the health care industry" for the protection of identifiable health information.

HHS also makes the following significant findings:

1. "...security and privacy are inextricably linked. The protection of the privacy of information depends in large part on the existence of security measures to protect that information." 68 Fed. Reg. at 8335.

2. "...a number of implementation specifications are so basic that NO COVERED ENTITY COULD EFFECTIVELY PROTECT ELECTRONIC PROTECTED HEALTH INFORMATION WITHOUT IMPLEMENTING THEM." Id.

3. "THESE PROTECTIONS ARE NECESSARY TO MAINTAIN THE CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY OF PATIENT DATA. A covered entity that lacks adequate protections risks inadvertent disclosure of patient data, with the resulting loss of public trust, and potential legal action. For example, a covered entity with poor facility access controls and procedures would be susceptible to hacking of its databases." 68 Fed. Reg. at 8,344.

4. "Whether or not to implement [the Security Standards] before the compliance date [April 21, 2005] IS A BUSINESS DECISION THAT EACH COVERED ENTITY MUST MAKE." 68 Fed. Reg. at 8,362.

Thus, statements by HHS accompanying the new Security Standards rule acknowledge that the privacy of the identifiable health information that the Privacy Rule gives regulatory permission for covered entities to use and disclose, cannot be protected for at least two years after the

compliance date of the amended Privacy Rule. HHS further acknowledges that the failure to implement such protections will result in destruction of the public's trust in the nation's health delivery system.

Further, the final Security Standards Rule acknowledges that, even if they were implemented on the compliance date, the Security Standards will not protect the privacy of the information that covered entities are authorized to use and disclose under the amended Privacy Rule. First, the Security Standards do not apply to the same information as is covered by the Privacy Rule: "...this final rule requires protection of the same scope of information as that covered by the Privacy Rule, EXCEPT THAT IT ONLY COVERS THAT INFORMATION IF IT IS IN ELECTRONIC FORM. We note that standards for the security of all health information or protected health information in nonelectronic form may be proposed at a later date." 68 Fed. Reg. at 8,342.

Second, HHS agrees "that there is no such thing as a totally secure system that carries no risk to security." 68 Fed. Reg. at 8,346. Thus, HHS has stripped consumers of the power to exercise their own right to medical privacy by eliminating the right of consent and has failed to provide privacy protections that will prevent this information from being improperly used and disclosed. Further, HHS acknowledges that there are no privacy protections that are as effective as allowing the individual to refuse the use and disclosure of his identifiable health information.

Finally, HHS also notes "some form of sanction of punishment activity must be instituted" in order for the statutory requirement for safeguards to be implemented. 68 Fed. Reg. at 8,346. However, no sanction or punishment regulations have even been proposed for the amended Privacy Rule.