McKesson Provider Technologies – Medical Imaging Business Unit
#130-10711 Cambie Road
Richmond, BC
Canada V6X 3G5
604.279.5422 Tel
604.279.5468 Fax

McKESSON
Empowering Healthcare

December 2, 2004

Marietta L. Squire
Committee Management Spec.
OCD/CPHDSS
CDC/National Center for Health Statistics
3311 Toledo Road, Rm. 2340
Hyattsville, MD 20782

By email: mrawlinson@cdc.gov

Re: Supplemental Testimony from McKesson Provider Technologies Medical Imaging business unit per November 19, 2004 meeting of NCVHS Subcommittee on Privacy and Confidentiality

Dear Ms. Squire:

McKesson would like to thank the Subcommittee for the opportunity to present testimony on the issue of HIPAA security and Medical Device regulation. Based on the Subcommittee's response and the questions raised during the panel testimony, McKesson would like to supplement its testimony as follows:

1. Mandatory use of the HIMSS Manufacturer Disclosure Statement for Medical Device Security (MDSMDS)

   While McKesson agrees that some form of standardized means to keep medical device users informed as to the status of their devices with regards to the HIPAA security provisions, mandating the use of the MDSMDS has certain shortcomings in McKesson's view:

   a. As presently drafted, it covers only a small portion of the HIPAA requirements applicable to many devices. Thus, for example, while the MDSMDS simply asks whether a password is required to access the device, the security requirements that may be applicable to a device may be more extensive than that, and the detail required for the user to evaluate the security risk presented by the device may be more extensive than a simple "Yes/No." McKesson has developed and provides its customers with access to a single document describing the device's compliance in a number of HIPAA-related areas (e.g. Code Sets, Transactions, Privacy, and Security regulations); in our opinion, the maintenance of a separate document that addresses only a subset of the HIPAA requirements could be burdensome as well as potentially confusing to the user. [We can make a copy of the McKesson document available to the Subcommittee at their request.]

b. With the compliance date of April 21, 2005 fast approaching, there may be inadequate time for the device manufacturers to prepare and make available the completed forms such that the users can utilize the information.

c. A comparison of the MDSMDS with HIPAA questionnaires from health care facilities completed by McKesson indicates that health care facility questionnaires request more specific details than is included in the MDSMDS. Thus, even if the MDSMDS is mandated, it is very likely that health care facilities would still request medical device manufacturers to complete their own "supplemental HIPAA questionnaires".

Therefore, if the Committee mandates the use of a questionnaire, McKesson believes that it is imperative such form be the exclusive means for documenting the compliance statute of medical devices. Otherwise, manufacturers will expend time and resources in preparing the forms only to have the users request that their own particular form or survey be completed. Thus, any expected efficiency of communication would be lost and the potential for conflicting information and misinterpretation would be compounded.

2. There was much discussion of the risks and benefits of "hardening" medical devices against viruses, intrusion attacks, etc. Given the sheer number of "legacy" devices in use today and the relatively short timeframe remaining to complete compliance efforts, McKesson believes that efforts would be more appropriately focused on "hardening" the **network environments around the devices** rather than the medical devices themselves. Simply put, it may be much more time-effective (and cost-effective) for institutions to "harden" the environment around the legacy devices through improvements in network security and alterations in their administrative procedures.

Many user institutions have on-going projects related to system and infrastructure security; even if manufacturers could provide "retrofits" for the legacy devices, users may not have the resources to apply and test individual patches to individual devices without pulling those resources from the larger infrastructure security projects that will have the benefit of preventing access or intrusion to all the devices within the infrastructure.

Requiring device manufacturers to provide "retrofits" to legacy devices was also discussed at the hearings. McKesson believes that such a requirement would be ill-advised, particularly for those devices that may no longer be in production. In many cases, newer devices have been introduced to take advantage of technology improvements, including improvements in security-related functionality and to "retrofit" those changes to devices no longer in production may not even be possible because of discontinuance of support from third party vendors for the incorporated products. Again, McKesson notes that even if a requirement for such retrofits to be made by device manufacturers were to be promulgated, it is highly unlikely that manufacturers could even design and produce the "retrofits". Further, it is almost certain that the user community would have little or no opportunity to implement the changes, by the April 21, 2005 compliance date.

If you have any questions regarding our supplemental information, please do not hesitate to contact me. Thank you again for the opportunity to provide our perspective on this critical issue.

Best Regards,

McKesson Provider Technologies

Robert MacNeil, P.Eng
Manager, Quality and Regulatory Affairs