APPENDIX 2

AN EXAMPLE OF THE SCALABILITY OF THE SECURITY STANDARD

Large Practice

- Security official should be someone other than one of the doctors or the practice manager. This person should be dedicated to the role of the security official. May be the same person as the privacy official.
- Consider using biometric identifiers to access network
- 128 bit encryption should be in place (symmetric, private, public keys)
- Robust firewall (theoretically with a built in virus protection protocol)
- Should implement specific access control software to manage users of the network
- Should implement specific access control software to audit user access on the network
- Should create an incident database to log events within the network.

- Token or Smart Card for authentication/access control
- Automatic Logoffs
- 64 bit encryption
- Virtual Private Network (VPN) technology

- Security official can be the office manager as well. Individual does not need to have the sole responsibility of the Security Officer.
- User I.D. and password protection to network
- User access log
- Anti-viral software in place
- Inexpensive firewall software in place
- Establish levels of authorization.
- Password protected Screensaver
- 32 bit encryption (Note: Most PMS/EMR software has built in 128 bit encryption)
- Simple audit processes provided by PMS.

Small Practice