

MUSC
Data Transmission over the Internet
Policy Statement and Procedure

Policy Statement:

In accordance with HCFA's Internet Security Policy issued 11/24/98 (see <<http://www.hcfa.gov/security/isecpolicy.htm>>, all HCFA Privacy Act including patient identifiable data must meet HCFA requirements, including encryption and authentication, when being transmitted over a public network or the Internet. Please note that this policy does not apply to non-identifiable patient data.

Procedure:

1. Review HCFA Internet Security Policy for privacy requirements (see above web address).
2. Users requesting transmission of data over the Internet must first complete the Internet Transmission of Patient Identifiable Data Request Form (Form # ISO-01) and submit to the MUSC Information Security Officer.
3. The request will then be forwarded to CCIT and will undergo review and technical testing by a representative task force at CCIT.
4. Approval and/or recommendations from the CCIT task force will be forwarded to the Information Security Officer.
5. The Information Security Officer will present the request and CCIT review to the MUSC Security and Confidentiality Committee for approval. If a request is not approved the requestor will receive recommendations from CCIT and the Security and Confidentiality Committee and may re-apply for transmission once those requirements are met.
6. Approved requests will be forwarded to the Vice President of Medical Affairs for final approval.
7. Additional testing may be scheduled as necessary.
8. Requestors are responsible for maintaining their system's security controls, and for making any changes warranted by evolving technical and/or regulatory requirements. The Information Security Officer will assist in this process by sending notifications of regulatory changes to Requestors; re-certification of systems may be required.
9. All approved systems are subject to periodic internal audits, as well as to HCFA audits should they occur.