Policy and Procedure: HIPAA/HITECH Compliance
Topic: *Acceptable Encryption*

Policy Purpose:

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. In addition, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

Policy Description / Responsibilities:

Industry standard algorithms such as DES, Blowfish, RSA, RC5, and IDEA will be used as the basis for encryption technologies. Symmetric cryptosystem key lengths must be at least 56 bits. Asymmetric cryptosystem keys must be a length that yields equivalent strength. Saratoga Bridges' key length requirements will be reviewed annually and upgraded as deemed necessary by the IT/IS department based on technology, best practice, legal requirements and ROI.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by IT. Be aware that the export of encryption technologies is restricted by the U.S. Government. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.