Scope
This policy applies to the College of Dentistry’s protocol to encrypt Protected Health Information (PHI).

Policy
The U.S. Department of Health and Human Services (HHS) Office for Civil Rights announced a final rule that implements a number of provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, to strengthen the privacy and security protections for health information established under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

One of the provisions of the HITECH act is that all mobile data devices used to access or store Protected Health information (PHI) must be encrypted. Encryption is a way to enhance the security of data by scrambling the contents so that it can be read only by someone who has the right encryption password, pin or key to unscramble it.

The College of Dentistry’s policy is that encryption is required on all collegiate purchased desktops, laptops, flash drives, portable hard drives and all other mobile devices and peripherals, regardless if the device contains PHI or not. This includes all desktop computers purchased with University funds and used at home.

All personal devices that are used to access or store PHI data must also be encrypted. This includes desktops, laptops, flash drives, portable hard drives and all other mobile devices and peripherals. If an authorized user (faculty, staff or student) elects to place PHI data on a personally owned device, they are responsible for its security, confidentiality, and integrity and that the device has been properly encrypted. The user is personally responsible for any breaches that occur as a result of his/her noncompliance of this policy.

In addition to encrypting devices, all laptop and home computer user accounts must have a password that meets the University password policy on complexity and length. A screensaver must also be enabled.
and wakeup from it must require a password. All smartphones and tablets, whether owned by the
University or by you personally, that are used to access University email, must be password protected.

All new University purchased devices will be encrypted prior to deployment to the end user. All existing
University and personal devices that fall under this policy will need to be encrypted by September 1,
2014. Faculty, staff and students are instructed to contact the Dentistry Help Desk to get their University
owned device(s) encrypted. Encryption for personal devices that fall under this policy is the
responsibility of the device owner. The links below will help you encrypt your device. If you need
assistance encrypting your device, contact the Dentistry Help Desk.

Types of Encryption used:
1. All Windows devices will be encrypted using Dell Data Protection or Bitlocker.
2. All Mac devices will be encrypted using Dell Data Protection or FileVault.
3. If these encryption methods do not work on a specific device, we will try to encrypt it with
another suitable application.
4. If a device cannot be encrypted for technical reasons, then you cannot store PHI data on it.
   There will be no exceptions to this rule.

Encryption keys will be managed and protected by the following:
1. Recovery keys for University owned computers (desktops, laptops, etc.) will be stored in the
College of Dentistry computer database.
2. Recovery keys for University owned flash drives will be stored on the College of Dentistry share
   drive.
3. Recovery keys for personal devices are the responsibility of the device owner. If a device
   password and recovery key are lost, the data on the device is permanently lost. The only way
   the device can be used again is to reformat it, which wipes the device clean. Never store your
   only copy of important data on a flash or removable drive.

Anyone found not in compliance with this policy is subject penalties levied by either the College of
Dentistry, the Federal Government or both. If the violation results in a breach of PHI, the College of
Dentistry’s HIPAA penalty grid will be used. Federal fines are at the discretion of the Government. If the
violation does not result in a breach but is a violation of policy, then reprimand will follow University
Human Recourses progressive discipline guidelines, which include termination.

Any lost or stolen device must immediately be reported to the Technology and Media Services Director.

Resources
§ 164.312 Technical safeguards

University of Iowa Enterprise Password Policy
http://its.uiowa.edu/hawkid/password

Bitlocker Overview
How to encrypt your device using Bitlocker
http://windows.microsoft.com/en-us/windows/protect-files-bitlocker-drive-encryption#1TC=windows-8

FileVault overview and how to encrypt your device using FileVault
http://support.apple.com/kb/ht4790