THE UNIVERSITY OF ARIZONA

HIPAA Privacy Program Guidance: Methods for Securely Emailing PHI or IIHI

PURPOSE

To provide guidance about methods for securely emailing Protected Health Information (PHI) at the University of Arizona.

REVIEW/REVISIONS

- 02/2016

DEFINITIONS AND RELATED INFORMATION

Individually Identifiable Health Information (IIHI): Information created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) that identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Protected Health Information (PHI): Individually identifiable health information transmitted or maintained in any form by a Covered Entity or Business Associate (exceptions, including employment records and records covered by FERPA, listed at 45 CFR § 160.103).

PHI includes: names (including initials); geographic information (address, ZIP, etc.); dates (birth, death, admission); numbers (Medical Record Number, Social Security Number, phone, fax, account number, etc.); email/web addresses; biometric identifiers (voice, finger prints); full face photographs or comparable images (tattoos, etc.); any other characteristic that could uniquely identify the individual.

FOUR METHODS FOR SECURELY EMAILING PHI OR IIHI

1. Completely de-identify the data before emailing by removing all PHI identifiers (see above).

2. Encrypt the email.
    a) Emails sent/received within and between Banner and University of Arizona Health Sciences (UAHS) email addresses (e.g., aemrc.arizona.edu, anesth.arizona.edu) are secure.
    b) Emails sent from an arizona.edu email address to a non-university email address (e.g., Gmail) can be encrypted by typing **[encrypt]** or **[secure]** in brackets in the subject line of the email. *These commands are case sensitive.*

3. Password-protect all attached documents (e.g. Word, Excel, .PDF) that contain PHI or IIHI, and provide the password to the recipient in a *separate* Email.

4. Digital Certificates: Emails sent/received from an arizona.edu email address to another arizona.edu address cannot be encrypted per 2(b), and may not otherwise be secure. Please install (or, preferably, ask your IT staff to install) digital certificates with encryption capability on *all* of your devices. Information about obtaining a digital certificate can be found here: http://uits.arizona.edu/services/email/digital-certificates