HIPAA Security Tip Considerations Prior to Study Submission in the ePirate Portal
Prepared by ECU IT Security

Prior to submitting your study into the ePirate Portal for IRB review, you should be aware of ECU HIPAA Policies which affect the electronic storage of research data. If any of these items are not addressed prior to submission, it will cause your submission to be returned and significantly prolong the IT Security approval process of your study. IT Security has very limited resources and is unable to quickly respond to incomplete and inaccurate submissions. To expedite your study approval in IT Security, consider the 8 items below and answer completely all the appropriate questions in Section 11.1 Information Technology Security for Protected Health Information at ECU/BSOM in ePIRATE.

1) According to HIPAA Security Policies #8 and #16 on the HIPAA Security Website (www.ecu.edu/HIPAA), electronic Protected Health Information (ePHI) stored on workstations or portable devices must be encrypted. All 18 identifiers must be removed in order to not be subject to HIPAA policies. This includes the temporary storage of ePHI before extracting data for your study such as from a survey, medical record, or interview.

2) Storing ePHI on a password protected laptop/workstation does not meet HIPAA policy requirements. IT Security suggests the temporary storage of data on Piratedrive, encrypted storage on workstation or encrypted flash drive while the study data is extracted, and then delete the ePHI as soon as possible after study data has been extracted. Document in Question #4 in Section 1 of the Information Technology Security for Protected Health Information at ECU/BSOM (Section 11.1 in ePirate) the temporary storage location and how long the data will remain in that location before it is deleted. Please contact the ECU Help Desk at 328-9866 or www.ecu.edu/9866/ for assistance with encryption on workstations or encrypted flash drive recommendations.

3) If you have determined that PHI cannot be de-identified by the removal of all 18 personal identifiers as noted by HIPAA Privacy De-identified Policy #13 (http://www.ecu.edu/cs-dhs/hipaa/privacy/policies.cfm), then your study data will be classified as a HIPAA System by ECU IT Security. If you have questions regarding the 18 identifiers, please see Attachment 1 for the 18 identifiers, HIPAA Privacy De-identified Policy #13, or contact the HIPAA Privacy Office.

4) An Administrator of a HIPAA system must be named as the responsible party in Question #3 of Section 3 in the Information Technology Security for Protected Health Information at ECU/BSOM (Section 11.1 in ePirate) to ensure appropriate security controls are implemented. The administrator will be required to prepare annual HIPAA system documentation including a Risk Assessment, and complete annual HIPAA Administrator Training.

5) All HIPAA systems must be documented, tracked and audited annually and the audit report will be submitted to the Health Science Vice Chancellor as required by ECU Policy. If you have questions regarding HIPAA Administrator Requirements, please contact ITSecurity@ecu.edu.
6) IT Security recommends **de-identified data be stored on ECU devices which have been approved by ITCS**. Please review Attachment 2, ITCS HIPAA and SSN Acceptable Storage Device List or visit the IT Security website at this link ([http://www.ecu.edu/cs-itcs/itsecurity/upload/ITCSSensitiveDataAcceptableStorageDeviceList.pdf](http://www.ecu.edu/cs-itcs/itsecurity/upload/ITCSSensitiveDataAcceptableStorageDeviceList.pdf)).

7) If you are storing **HIPAA data on paper documents, document the security controls for protecting the paper documents and limiting access to only those who are authorized to the ePHI**. Examples of security controls include but are not limited to: storing under lock and key, and tracking of who has access in the form of a log.

8) If HIPAA Privacy approves the storage or transmission of ePHI to an external entity, indicate in Question #6 in Section 3 of Information Technology Security for Protected Health Information at ECU/BSOM (Section11.1 in ePIRATE). Please review Attachment 3, Data Transmission Security Checklist for transmissions options.
Attachment 1

De-identification of PHI

Covered entities may use or disclose health information that is de-identified without restriction under the Privacy Rule. Covered entities seeking to release this health information must determine that the information has been de-identified using either statistical verification of de-identification or by removing certain pieces of information from each record as specified in the Rule.

The Privacy Rule allows a covered entity to de-identify data by removing all 18 elements that could be used to identify the individual or the individual's relatives, employers, or household members; these elements are enumerated in the Privacy Rule. The covered entity also must have no actual knowledge that the remaining information could be used alone or in combination with other information to identify the individual who is the subject of the information. Under this method, the identifiers that must be removed are the following:

1. Names.
2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP Code, and their equivalent geographical codes, except for the initial three digits of a ZIP Code if, according to the current publicly available data from the Bureau of the Census:
   a. The geographic unit formed by combining all ZIP Codes with the same three initial digits contains more than 20,000 people.
   b. The initial three digits of a ZIP Code for all such geographic units containing 20,000 or fewer people are changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
4. Telephone numbers.
5. Facsimile numbers.
6. Electronic mail addresses.
7. Social security numbers.
8. Medical record numbers.
9. Health plan beneficiary numbers.
10. Account numbers.
12. Vehicle identifiers and serial numbers, including license plate numbers.
15. Internet Protocol (IP) address numbers.
16. Biometric identifiers, including fingerprints and voiceprints.
Attachment 1

17. Full-face photographic images and any comparable images.
18. Any other unique identifying number, characteristic, or code, unless otherwise permitted by the Privacy Rule for re-identification.

Re-identification: The covered entity may wish to re-identify information previously de-identified, but is not required to do so. This re-identification may be accomplished through the use of a unique code, key or other means of record identification, provided that the following specifications are met:

- Code Origin. The code, key or other means of record identification is not derived from or related to the PHI about the individual, and is not otherwise capable of being translated so as to identify the individual. In other words, the unique code, key or record identifier must not be such that someone other than the covered entity could use it to identify the individual (such as a derivative of the individual’s name or social security number.)
- Code Security. The covered entity does not use or disclose the code, key or other record identifier for any other purpose, and does not disclose the mechanism for re-identification. The code, key or other record identifier must be kept confidential and secure.

If PHI cannot be de-identified, HIPAA Privacy and Security controls must be implemented.
ITCS SENSITIVE DATA ACCEPTABLE STORAGE DEVICE LIST

Storage of HIPAA and SSNs outside of the official EMR or Banner System must be approved prior to storage. For HIPAA storage, please submit a Help Desk request at https://ithelp.ecu.edu/ or at 252-328-9866. For SSN storage, please submit a SSN Use, Disclosure and/or Storage Request Form to ITPC@ecu.edu.

Acceptable Storage Devices
1. ECU Official EMR Systems
   a. Centricity
   b. HealthSpan

2. ITCS Server Certified for HIPAA Storage
   a. If you have not confirmed with ITCS that your server solution meets HIPAA Security requirements, contact ITCS Helpdesk at 252-328-9866 for consultation with IT Security.

3. Departmental Server Certified for HIPAA Storage
   a. If you have not confirmed with ITCS that your server solution meets HIPAA Security requirements, contact ITCS Helpdesk at 252-328-9866 for consultation with IT Security.

4. ECU Pirate Drive
   a. If you are the only person required to access the research, then storage can occur on your personal Pirate Drive space. If you are required to share research with others or multiple people will be managing multiple research projects, the use of a departmental Pirate Drive is highly recommended. Visit the Pirate Drive information webpage and contact ITCS Helpdesk at 252-328-9866 to request the creation of a departmental Pirate Drive space.

5. Encrypted Hard Drive
   a. Check the ITCS Encryption webpage for encryption options and contact the ITCS Helpdesk at 252-328-9866 to request a hard drive encryption solution.
DATA TRANSMISSION SECURITY CHECKLIST

1. Secure File Transfer (SFTP)
a. You must work with your data recipient to ensure they have the capability to receive files via SFTP. Contact the ITCS Helpdesk at 252-328-9866 for assistance with setting up a SFTP solution.

2. Encrypted Web Portal
a. Only if you are authorized from HIPAA Privacy to store the ePHI external to ECU.

3. Encrypted Portable Device
a. 256-Bit Encrypted Device (e.g. Ironkey encrypted flash drive)

4. Email Options (NOTE: email is NOT an acceptable solution UNLESS you encrypt the email message)
a. Encrypt the file attachment containing sensitive data. WinZip or TrueCrypt are recommended solutions.
b. Encrypt the email containing sensitive data. IronPort Encryption is a recommended solution. You are required to purchase the IronPort Encryption license if your department does not already own the license key. Check with your departmental administrator. Contact the ITCS Helpdesk at 252-328-9866 if your department does not own a license and you need additional information on purchasing one.