What is PHI?

HIPAA Security regulations define Protected Health Information (PHI) as any information, whether oral or recorded, in any form that is created or received by a health care provider, health plan, employer, insurer, school or university, health care clearinghouse or a business associate; and relates to the past, present, or future, physical or mental health or condition, provision of health care, or health care payment of an individual.  Learn about the 18 PHI identifiers

WHERE CAN I STORE PHI?  DID YOU KNOW?

Q: Can I save Protected Health Information (PHI) on my personal device (USB flash drive, external hard drive, home computer, iPhone, iPad, etc.) to work on from home, perform research or share with my colleagues?

A: No. PHI must only be stored on university-approved and authorized devices. If you are unsure if a device is university-approved, contact ITSecurity@ecu.edu.

Placing Protected Health Information such as a patient’s name, medical record number, birth date, and related information on your personal USB flash drive is a HIPAA violation. Loss of that flash drive would threaten the privacy and safety of patients.

Violation of HIPAA laws could lead to ECU being fined up to $1.5 million dollars and possible individual criminal penalties (including imprisonment).

If you think it’s critical to store patient data on a flash drive, please contact ITSecurity@ecu.edu.

HIPAA SECURITY IN THE NEWS

State Pays $1.7 Million for Lost Hard Drive

The State of Alaska announced in June 2012 that it is paying $1.7 million to the federal government for a 2009 security breach of patient data. A federal investigation following the breach found inferior security measures in place at Alaska’s Department of Health and Social Services. In October 2009, a portable hard drive was stolen from the car of an employee who worked for the State Health department.  Read more about the security breach