Vanderbilt University Medical Center

Privacy and Information Security Training –

Information Privacy & Security Website:

Information Privacy and Security

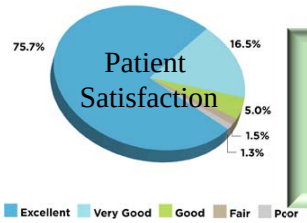
VANDERBILT UNIVERSITY
MEDICAL CENTER

Respect for Privacy and Confidentiality

It's the right thing to do

It's a VUMC Credo Behavior

MyVUMC
VANDERBILT UNIVERSITY MEDICAL CENTER



It's a key driver to overall patient satisfaction

It's the Law!!!

U.S. Department of Health & Human Services
HHS.gov

WHAT PARTS OF RESEARCH ARE INSIDE THE HEALTHCARE COMPONENT OF THE HYBRID ENTITY?

INSIDE THE HEALTHCARE COMPONENT

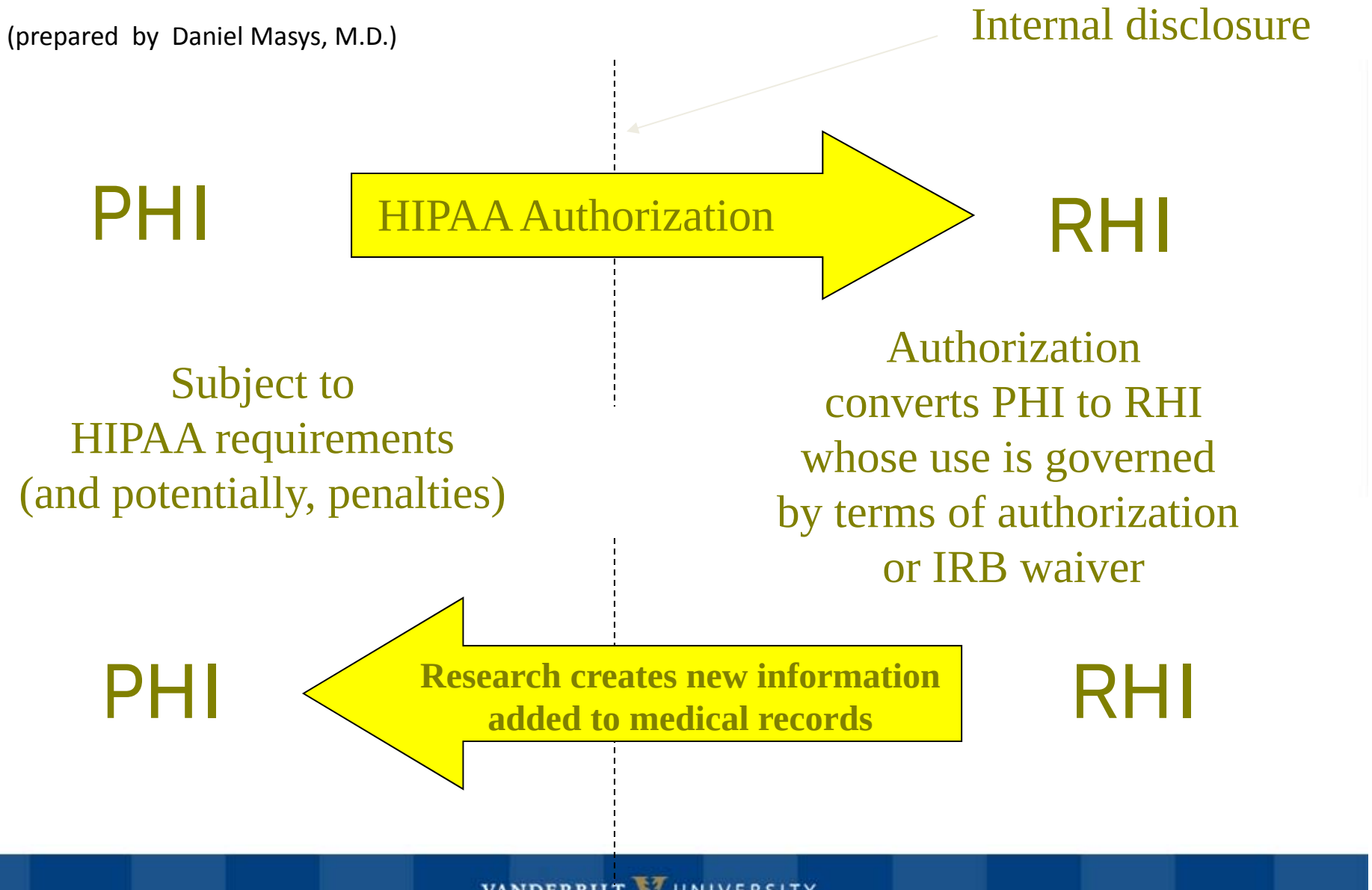
- **PHI is health information created, used, and/or stored as a by-product of the delivery of health care services (stored in the designated record set)**
- **Human Subjects Research using PHI**
- **Clinical Trials**
- **Health Information created as RHI and conveyed to the medical record to support treatment purposes**

OUTSIDE THE HEALTHCARE COMPONENT

- **Research Health Information is created, used, stored, or disclosed from a research data file or system distinctly separate from the patient's medical record**
- **Animal and Basic Sciences Research**
- **Human Subjects Research not using PHI**

PHI <-> RHI

(prepared by Daniel Masys, M.D.)



Data Handling Implications for PHI vs. RHI

- PHI is subject to the HIPAA for the Privacy Rule and the Security Rule.
- RHI is subject to best practices for maintaining confidentiality of research records, but not subject to HIPAA.
- Subsequent uses and disclosures of RHI are governed by the terms of the authorization or waiver, not by HIPAA.

Uses and Disclosures for Research

HIPAA and VUMC policy generally limit the use and disclosure of PHI to treatment, payment, and administrative operation (TPO) functions, unless proper authorization is secured from the patient. Research falls outside of TPO and will always require specific authorization or other protections.

PHI can be used or disclosed for research purposes if one of the following conditions is met:

- With a specific authorization signed by the patient
- With an IRB waiver of this authorization
- Under the "Preparatory to Research" criteria in IRB Policy X.A
- As a limited data set in conjunction with a Data Use Agreement
- As fully de-identified data
- For research on decedents
- Disclosures related to FDA-regulated products.

Careless Handling of Patient Information

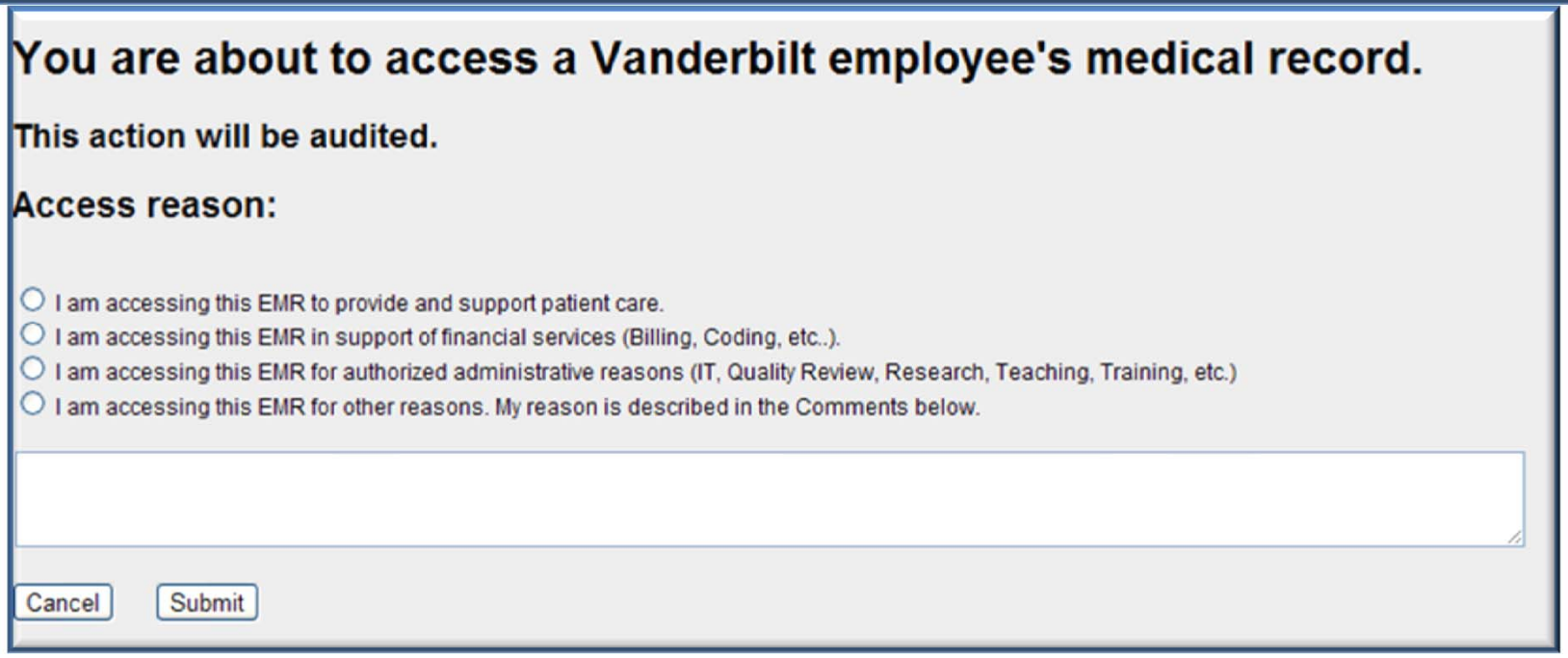
Things You Need to Know:

- When mailing patient information always ***double check*** to be sure you are sending the correct patient's information to the correct person at the correct address.
- Be sure to ***verify*** that you are giving the correct patient the information belonging to that patient.
- When faxing a document always use a cover sheet that includes the sender's full name, department or clinic name, and complete phone number and fax number. ***Double check*** and ***always confirm*** to be sure you are sending the right patient's information to the right recipient at the confirmed fax number.
- When you select a recipient for faxed documents from StarPanel Provider Communication Wizard always confirm that you have the correct provider by name, specialty, office location, and fax number.
- When looking for a patient's medical record, attempt to use more than first and last name to identify the correct patient; e.g. birth date or middle name
- MyHealthatVanderbilt is a secure web portal that can be used as an alternative to email and faxing when communicating with patients.
- Avoid conversations about patients in an area that is open to the public where you might be overheard.
- Written documentation or printed documents that contain VUMC Protected Health Information ***MUST*** be placed in a shredder bin or processed through a shredding device (preferably a cross-shredder). Shredder bins are located throughout the Medical Center.

Key Point – Auditing

Accessing a patient's Electronic Medical Record (EMR) other than for job related reasons or without written authorization from the patient is unacceptable. If the patient is a VUMC employee and an attempt is made to access that employee's record; you will see the screen below the 1st time you access the EMR.

If the EMR is not accessed within 14 days, you will be prompted again to give an access reason.



Sharing Passwords and Using Someone Else's User ID

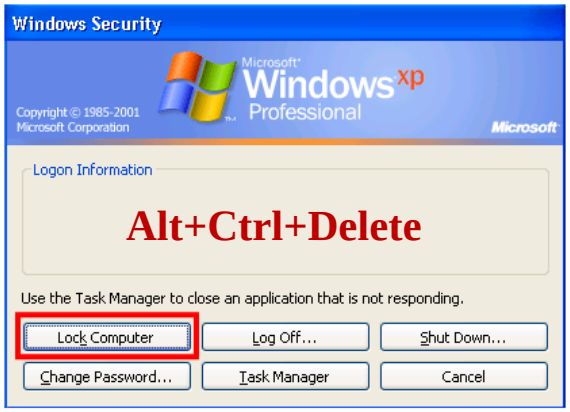
Individual user identification is essential to maintaining the accuracy, integrity, and confidentiality of the electronic information systems and the patient's medical record.

Most Frequently Reported Incidents

- Staff or faculty member logs onto electronic workstation in a shared work area and leaves the device allowing others to access patient information under the user identification first used.
- Staff or faculty member accesses electronic patient information without first logging on with their own unique identification.
- Staff or faculty member shares their own unique User ID and Password that allows access to restricted systems and or confidential information or PHI of others.
- Staff or faculty member shares User ID and Password that allows access to that individual's computer or personal information, not to restricted systems or confidential data.

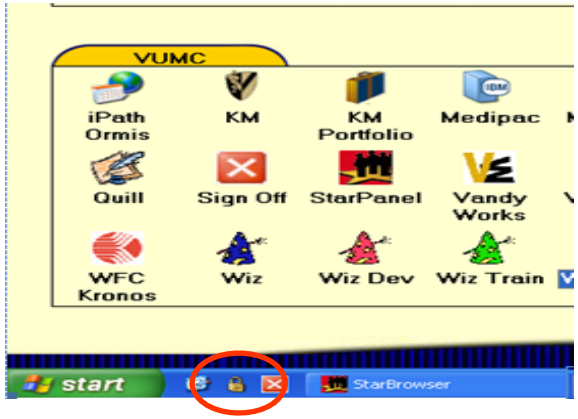
Key Point – Locking Workstations

If you are working on a *Administrative Workstation*(AWS) hold down the Alt, Ctrl, and Delete button simultaneously and click on Lock Computer.



When you return to your AWS, repeat the same steps, Hold down the Alt, Ctrl, and Delete button at the same time. You will be prompted to key in your password.

To Lock a *Clinical Workstation* (CWS) without losing any data, find lock image near Start box in lower left corner of task bar. Click on lock.



When you return to your CWS, click the Esc key as if you are doing a complete sign on. Note that your User ID will already appear in the box so you can reactivate your session by entering just your password

If you fail to log off a computer or lock the screen and someone uses the computer under your user identification, you may be held accountable for any resulting activity (e.g., unauthorized access to a patient's record, inappropriate use of the Internet).

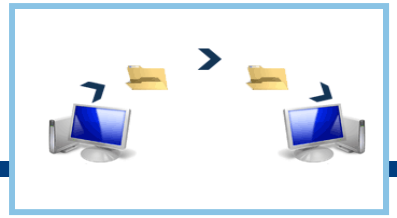
Electronic Communications and Information Technology Resources

Things You Need to Know:

- If you identify yourself in any online forum as a faculty/staff member of VUMC or use your Vanderbilt email address, you **must** make it clear you are not speaking for VUMC and all submissions represent your own personal views and comments.
- **Do not** post digital images and messages containing protected health information (PHI) without written authorization from the patient. **Remember** recognizable markings or body parts are PHI.
- Remember that all content contributed on all platforms becomes **immediately** searchable and can be **immediately** shared…It **immediately** leaves your control forever.
- Known or suspected incidents involving use or disclosure of PHI or Personal Information through social networking are reported to the VUMC Privacy Office and investigated.
- Federal law and regulations require **breach notification and reporting** when a patient's health information is accessed, used or disclosed in a way that violates the Privacy Rule of HIPAA and poses a significant risk of reputational, financial, or other harm to the individual.

Reference HR-025: *"Electronic Communications and Information Technology Resources Policy"*

File Transfer Application (FTA)



*FTA is an application that allows the user to send a secure **ATTACHMENT** that contains PHI, RHI or sensitive information. The information typed in the body of the email is not secure, **ONLY THE ATTACHMENT**. USE one of the following methods to communicate patient and other confidential information: **FTA, De-identify, MHAV. Do Not send it in email!***

There are two types of FTA users - Web based and Outlook Plug-in:

- ***The Web Application user*** – a user whose position requires transfer of secure files internally or externally, ***less than 10 times per month***.
- ***The Outlook Plug-in Key Function User*** – a user whose position requires multiple occurrences of secure file transfers in ***excess of 10 times per month***.

Web Application Users – For Vanderbilt Users an account exists and logging in will activate the users account

- The User ID is the user's Vanderbilt email address
- The Password is the ePassword used with the users VUnetID
- After files are sent, ***Completely Close*** the Web Application (i.e. all Internet Explorer pages , windows and tabs)
- Access the link for more Web Application User information: File Transfer Application (FTA)

External Party receiving Information:

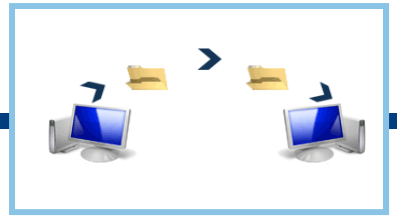
- The External user will receive an email from the Vanderbilt Workforce Member and will be required to set up an account for the Web Application.

Outlook Plug-In Users:

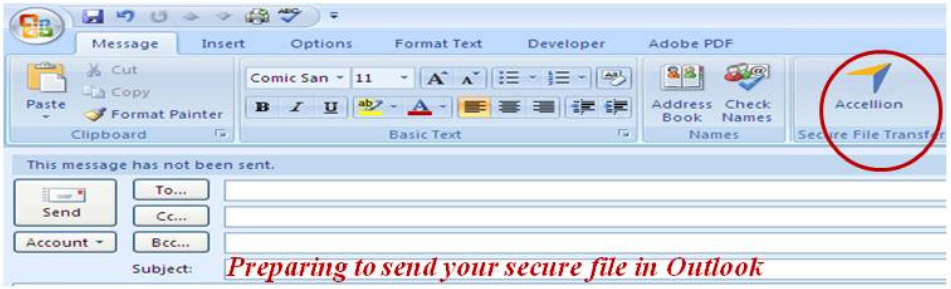
- Use of the Accellion Plug-In requires installation on the Vanderbilt user's workstation and will require assistance from the user's LAN Manager or Technical Support Provider
- Contact the Helpdesk (3-HELP) and request a ticket be sent to Network Security for installation of the Accellion Plug-In.
- Once the Accellion Plug-In is installed access the following link for directions: Outlook Plug-In Uses for Secure File Transfer

More Information on FTA may be found on the Information Privacy and Security Website: File Transfer Application (FTA)

File Transfer Application (FTA) Outlook Example

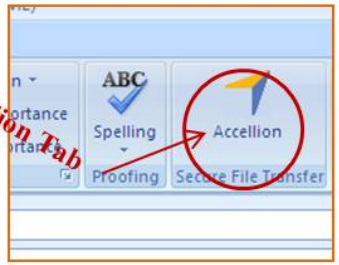


1

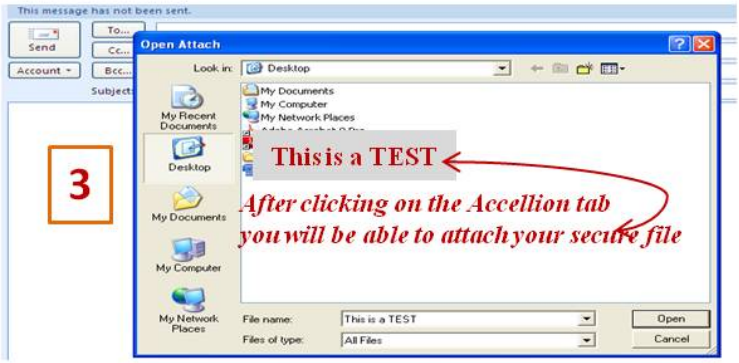


2

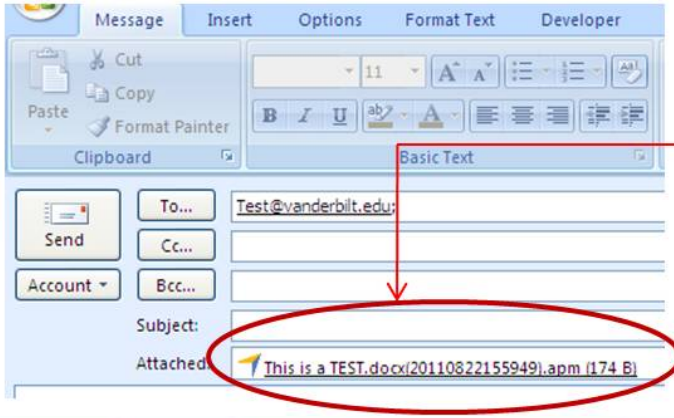
Click on Accellion Tab



3



4



The "*This is a TEST*" attached file is ready to be sent, and is secure. All information in the body of the email is not secure and should not contain any PHI, RHI or sensitive information.

Report Privacy Complaints or Suspected Violations to:

- Privacy Office (936-3594) or e-mail **Privacy.Office@vanderbilt.edu**

- Help Desk 343-HELP (343-4357)
- Compliance Reporting Line (343-0135)
- Always forward Patient privacy complaints to Patient Affairs (322-6154) or the Privacy Office.
- Your manager