

Communication Sciences and Disorders, Speech-Language-Hearing Clinic

Policies and Procedures

*REVISION DATE:*  August 14th, 2019

*SUBJECT:* **End Users IT Policy & Security #6**

Select Speech-Language-Hearing Clinic staff are responsible for auditing, processing and reconciling Clinic financial documents. Each of the below job functions are designed to give the least amount of access to potential HIPAA protected health information (PHI) while performing primary job functions. These job functions and their corresponding IT systems include:

Job Function: IT System:
- Creating Weekly Deposit Transmittals PS Financials
- Collecting & Processing Daily Revenue Deposits PS Financials
- Processing Expense Documents: Purchase Orders, PeopleSoft Financials
 Receivers, Journal Transfers, Check Requests
- Purchasing Card Approver and Reconciler PeopleSoft Financials
- Deposit/Revenue Collection Reconciliations PeopleSoft Financials &Enterprise Reports
- Monthly & Annual Budget Preparation PeopleSoft Financials &Enterprise Reports

Security Measures: In addition to HIPAA and university security policies, department end users will also note and adhere to the following:

* All emailed reports and documents that originate from the Clinic and all faculty and Clinical Supervisors and other NAU departments are to contain ***no*** PHI. If there are questions pertaining to the nature (PHI or not) of the information being sent via email, staff will error on the side of caution and ***not*** forward reports or documentation to any non-covered entity/staff. If a suspected breach has occurred, refer to the *Responding to Breaches of Protected Health Information (PHI)* on the NAU website,<http://nau.edu/Equity-and-Access/HIPAA/Policies/>, for what is/isn’t a breach and reporting requirements.
* Password Management: computer screens will be set to lock within 3 minutes of “idle” and/or when leaving ones desk/office.
* All Speech-Language-Hearing Clinic paper documents and files with potential PHI are stored in locking file cabinets in the Clinic office. Only the Administrative Associate and Insurance Billing and Collections Specialist have keys to the file cabinet.
	1. Weekly Revenue Deposits: Completed weekly deposit packets are saved and stored on a secure shares drive.
	2. Invoices: Paper invoices, after paid and scanned, are kept on file by vendor in the cabinet. Scanned invoices are stored in a secure shares drive.
* All HIPAA protected data will be purged (7) years after creation of the document. All other fiscal CSD and clinic documentation will be purged (5) years after creation of the document, per Arizona State regulations and document retention policy.

IT Hardware Removal Policy: In order to fully safeguard PHI (saved or cached) and make it impossible for recycled technology to be vulnerable to observation or theft, CSA IT staff will be notified to remove the following types of hardware & media from all CSD and clinic computer, tablets, etc. upon the end of the equipment’s lifecycle and/or upon releasing assets to property control:

* Physical Hard Drives
* Desktop & Laptop computers
* Tablets
* Thumb Drives or Key Drives
* Copiers/Scanner/Fax: When the department copier/scanner/fax (Konica Minolta Biz HUB) is removed and/or replaced, Konica Minolta will be contacted to re-image/wipe the hard drive of the machine. A Certificate of Completion of the hard drive re-image/wipe will be requested at time of removal.
* Employee Termination Process for IT: Upon general termination of employment, the following general tasks will be completed, including but not limited to:
* Notify CSA IT to…
	+ remove domain permissions to all Clinic and CSD share drives
	+ re-image the terminated employee’s workstation(s) and iPad (as applies)
* Notify Enterprise Reporting IT to…reporting@nau.edu
	+ remove access to all security roles
* Immediate Supervisor will initiate an ePASS to deactivate all PeopleSoft & HR security roles.