Electronic Record Security Standards Policies and Procedures
University of Alabama Counseling Center

1. Designation of Security Officer
The Director of the Counseling Center (CC) is designated as the Security Officer for the CC. The Security Officer is responsible for: (1) developing and overseeing CC security policies and procedures; (2) ensuring that each staff member understands his/her responsibilities and duties under the Security Rule and under these policies and procedures; and (3) ensuring that each staff member receives adequate training to comply with these policies and procedures.

2. Securing Your Office

Office Security Standard (Facility Access Controls)
The following policies and procedures apply to ensure the physical and technical security of the computers and portable electronic devices that are regularly used at the CC and that contain or process electronic protected health information (EPHI):

- **Contingency Operations (Addressable)**
The following policies and procedures apply to ensure that necessary CC operations can continue in the event of an emergency: CC staff members are the only persons who would need to access EPHI in event of an emergency. All employees have appropriate access to the office and computer system. CC staff may allow UA OIT staff into CC to recover EPHI in the event of an emergency. This determination will be made by the Director of CC or delegate.

- **Facility Security Plan (Addressable)**
The following policies and procedures apply to ensure the security of the office: Door locks on Suite 1000 of the South Lawn Office Building, offices, and windows are secure and of adequate strength and are maintained by Facilities and UAPD. Secure locks are also present on the file cabinets containing any portable electronic devices or other electronic media containing EPHI. After business hours, the CC is only accessible to CC staff and other authorized persons (UAPD and Facilities, including custodial staff). During business hours, staff monitors and controls access to areas where EPHI is present to prevent unauthorized access. Web-entry computers only allow students to submit information in data forms and allow no access to any other information within Titanium, the internet, or other University data systems. Written PHI is locked within cabinets at the end of each work day and computers are turned off or locked. After hours custodial staff is not authorized access to PHI in any format and are appropriately briefed on this expectation. Custodial staff is prohibited from logging onto CC computers. In addition, custodial staff network administrative permissions do not include access to EPHI which is only stored on the CC server, not on CC work stations. See also the section on “Securing Your Computer.”

- **Access Control and Validation Procedures (Addressable)**
The following policies and procedures apply to control access and to validate a person's identity in granting access to the office and computer systems based on his or her role or function (e.g., clients, employees, other visitors): All computers and software that may contain EPHI are password protected and login activity is monitored. The entire CC staff
monitors the Center, client and visitor movement and other activity to make sure that no unauthorized persons attempt to log onto CC computers. Visitors and other non-staff members (i.e., anyone who should not have access to EPHI) will not be left unmonitored in areas of CC in which these persons may intentionally or inadvertently gain access to EPHI. Any vendors or UA staff granted control and access to software programs for testing and revision purposes shall be monitored by CC staff, as appropriate. Web-entry computers only allow students to submit information in data forms and allow no access to any other information within Titanium, the internet, or other University data systems.

• Maintenance Records (Addressable)
  The following policies and procedures apply to ensure that the documentation of repairs and modifications to the physical components of the CC that are related to security is maintained. Not Applicable. These records are maintained by Facilities and Access Control.

Workstation (Computer and Electronic Device) Use and Workstation Security Standard
An inventory of computers and other devices is maintained by UA OIT. The Security Officer is responsible for ensuring the inventory is maintained and up-to-date. Physical access to all computers and other electronic devices will be maintained through the use of door locks on entrance doors to keep unauthorized persons from gaining access to EPHI. Computers and devices located in public areas of the CC are all to be situated so the screens of these devices do not face the waiting area where clients and other guests to the office are able to see what is on the screens. EPHI is not stored on computer hard drives or network drives other than the secure drive that houses the CC information management data base. Portable electronic devices and other electronic media containing EPHI are kept behind locked doors and in locked file cabinets and are not allowed off the premises. On the web-entry computers the USB ports and other CD or portable disk drives have been disabled to eliminate the possibility of unauthorized recording of the EPHI another student is entering.

3. Securing Your Computer

Access Control Standard
The following policies and procedures pertain to limiting physical access to computer systems and the office space or suite in which they are housed, while ensuring authorized access to the computer system and EPHI:

• Unique User Identification (Required)
The following policies and procedures apply to ensure that only authorized staff members can access the computer system and EPHI and that the authorized staff member is the person they claim to be. The CC complies with UA network security regulations. Each CC staff member has a unique user name and password for university network access as well as for access to the information management software. These user names and passwords must be used to have access to EPHI. EPHI is stored only on the CC server. Only CC staff can access the CC data base which is maintained by Titanium Software, via the administrative rights granted only to CC staff. Web entry computers have automatic log-on and only allow students to submit information in data forms and allow no access to any other information within Titanium, the internet, or other University data systems.
• **Emergency Access Procedure (Required)**
  The following policies and procedures apply to ensure that EPHI can be accessed in an emergency. The Security Officer will ensure that all EPHI necessary for daily operations is saved on a regular basis (e.g. daily). See also the section on “Data Backup Plan.” Such information includes client contact information, electronic mental health records, and the appointment calendar. If emergency access to EPHI is required (i.e. after hours), UAPD will contact the Director of CC or delegate to facilitate access to EPHI.

• **Automatic Logoff (Addressable)**
  The following policies and procedures apply to ensure that user computers are not subject to unauthorized access. In addition to the automatic locking feature that occurs at a five minute interval, users will manually lock their computers when they are away from their work area. The following location-specific expectations are in place:
  - In a continually staffed work area, users will manually lock their computers for extended absences (greater than 30 minutes).
  - Front office area computers will not be manually locked due to the potential interruption to daily work processes that such a feature would pose. The area is continually staffed during normal operating hours and has very limited access, minimizing the potential for unauthorized access.

Web entry computers have automatic log-on and only allow students to submit information in data forms and allow no access to any other information within Titanium, the internet, or other University data system. In the event of a safety drill or actual safety event that would require evacuating the building or that involved a break-in, staff will immediately manually lock their computers if reasonably able to do so and assuming it does not create undue risk to their own personal safety. The Security Officer periodically monitors computers in the clinic to ensure that users are locking their computers when required. CC staff members are required to log off of all software, external connections, and completely log out of the computer system at the end of the workday. Web-entry computers are logged off and shut down at the end of the day by CC staff.

• **Encryption and Decryption (Addressable)**
  The following policies and procedures apply to ensure that EPHI stored by the CC is encrypted so that it cannot be accessed by unauthorized parties.
  No EPHI is stored on individual workstations. EPHI is stored on the CC server or on portable or removable devices (e.g., external drives or USB devices). The CC server is located behind the Server Firewall to prevent unauthorized access. Only authorized CC staff can access the CC database. Note: The Titanium vendor can access the Titanium application/database located on the CC server for maintenance, troubleshooting, and other issues requiring access, when coordinated and facilitated by OIT staff. Titanium is HIPAA certified.

**Security Awareness and Training Standard**

• **Login Monitoring (Addressable)**
  The following policies and procedures apply to ensure that the Security Officer becomes aware of any unauthorized attempts to access the computer and EPHI. The CC server maintains a log file that ensures all access attempts to the server via user ID and password are logged for at least three weeks. These logs are periodically reviewed by OIT. Since users
do not log directly into the server, OIT would report unauthorized server login attempts found in the log to the Security Officer.

- **Password Management (Addressable)**
The following policies and procedures apply to ensure that CC staff appropriately create, change and safeguard passwords. Computer usage at CC is regulated by the University's OIT department. OIT requires use of "strong" passwords that meet the following three criteria:
  - Passwords must be at least eight characters long and contain at least one capital letter, one numeral, and one special character.
  - Passwords cannot be based on personal information about the individual (e.g., family or pet names) that would make it easy to guess a user’s password.
  - Passwords will be changed at least annually, as per CC policy. The CC Security Officer ensures staff compliance with this standard.

- **Protection from Malicious Software (Addressable)**
The following policies and procedures apply to ensure that unauthorized software that may contain spyware, adware or viruses that could compromise security is not intentionally or inadvertently installed on the computer system. OIT manages the CC computer system. OIT provides up-to-date virus protection software and regularly updates it. This software also checks all media and electronic attachments coming in from outside the system. OIT regularly updates various security features, security patches, or other software updates that are available to the computer operating system and all software programs that use or contain EPHI. Information Services takes steps to install the updates as soon as reasonably possible. CC staff members are prohibited from downloading software of any kind onto their computers without first consulting with OIT and the CC Security Officer. If the Security Officer becomes aware of the presence and operation of unapproved software on a CC computer, he will consult with OIT to make a determination as to whether or not this represents a Security Incident, and take steps accordingly. On the web-entry computers, USB ports and CD or other portable disk drives are disabled.

**Device and Media Controls Standard**
The following policies and procedures apply to ensure that CC monitors and controls the movement of electronic hardware and media containing EPHI into, out of, and within the office.

- **Disposal (Required)**
The following policies and procedures apply to ensure proper disposal or disposition of EPHI or hardware or media containing EPHI (e.g., discarding CDs containing EPHI, donating old computers to charity). Computers, devices and media containing EPHI can only be disposed of with the permission of, and at the direction of, the Security Officer. The Security Officer coordinates with OIT to ensure that all computer equipment and devices are disposed of in accordance with University policy and to electronic records compliant standards that ensure that EPHI cannot be accessed or recreated.

- **Media Reuse (Required)**
The following policies and procedures apply to ensure that storage media that may contain EPHI such as CDs, DVDs, USB devices, zip disks, tapes and diskettes are cleansed before reuse (e.g., all EPHI is completely removed). The CC Security Officer coordinates with OIT to
ensure that media containing EPHI is sanitized (e.g., all EPHI is completely removed) to electronic record compliant standards using a data destruction software program prior to reuse.

- **Accountability (Addressable)**
The following policies and procedures apply to ensure that there is a record of movement of any computers, devices, and media into and out of and within the office, and the staff members responsible for them. The Security Officer oversees the movement of all computers, devices and media into and out of (or within) the office, and the individuals or organizations responsible for safeguarding the device or media while outside the office. Activity regarding moving, destroying, or erasing computer hard drives are conducted and recorded by OIT. Computer devices are not moved internally or externally from CC without the knowledge and permission of the Security Officer. Staff must obtain permission from the Security Officer prior to removing any computers, devices and media from the office.

- **Data Backup and Storage (Addressable)**
The following policies and procedures apply to ensure that backup copies of EPHI are created and stored before computers and devices are moved. EPHI is stored on the CC server. See the “Contingency Planning Standard” in this policy for a description of backup and restoration plans.

**Audit Controls Standard**
The following policies and procedures apply to ensure that mechanisms are in place that record and examine access to the computer system and EPHI. The CC server maintains a log file that ensures all access attempts to the server via user ID and password are logged for at least three weeks. These logs are periodically reviewed by Information Services. Since users do not log directly into the server, Information Services would report unauthorized server login attempts found in the log to the Security Officer. The CC Security Officer, in consultation with OIT, and others as needed, will determine what actions, if any, need to be taken to minimize the potential for compromise of EPHI. See also “Security Incident Response and Reporting” in this policy.

**Integrity Standard**
These policies and procedures apply to corroborate that EPHI is not changed inappropriately or inadvertently.

- **Mechanism to Authenticate EPHI (Addressable)**
These policies and procedures apply to corroborate that EPHI stored by the CC has not been altered or destroyed inappropriately or without appropriate approval. The authenticity of mental health records is ensured through the administrative controls of the software vendor that CC uses, Titanium. The CC Security Officer is responsible for building the administrative controls in Titanium, which ensures that only appropriately licensed staff has administrative authority to sign records. Once a record has been signed, it cannot be altered and any changes to the record must be accomplished through an addendum or correction to the record, or a documented and saved request to unlock a note. Electronic records accuracy is monitored and evaluated internally through internal audits of mental health records.
Person or Entity Authentication Standard
The following policies and procedures are to ensure that persons or entities seeking access to CC EPHI are who they claim to be (e.g., a stranger is not attempting to log in as one of the CC staff). CC staff is small enough that the Security Officer is able to personally ensure that only bona fide CC staff members are working and able to access EPHI as authorized. In addition, staff members are required to change passwords at least annually. Passwords must contain at least eight characters, including at least one capital letter and one numeral. The University maintains and updates virus/firewall protection to prevent hackers from gaining access to its computers, according to currently recognized industry standards of protection.

Transmission Security Standard
The following policies and procedures apply to ensure that EPHI is only transmitted to the intended individual or entity and is not inadvertently or otherwise altered during the transmission outside the CC or over the internet.

- **Integrity Controls (Addressable)**
  These policies and procedures address the risk that EPHI could be improperly modified when transmitted through an electronic network. EPHI is stored on the CC server. The CC server is located behind the Server Firewall to prevent unauthorized access. Only authorized CC staff can access the CC database. Note: The Titanium vendor can access the Titanium application/database located on the CC server only with OIT facilitation. Titanium is HIPAA certified.

  The CC is not currently submitting insurance claims electronically.

- **Encryption (Addressable)**
  The following policies and procedures apply to ensure that EPHI transmitted electronically over open networks (e.g., the internet) is kept secure during the transmission process by encrypting it. EPHI is stored on the CC server. The CC server is located behind the Server Firewall to prevent unauthorized access. Only authorized CC staff can access the CC database. Note: The Titanium vendor can access the Titanium application/database located on the CC server only with Information Services facilitation. Titanium is HIPAA certified.

  The CC is not currently submitting insurance claims electronically.

4. Workforce and Administrative Policies

Security Management Process Standard (Sanctions and Review of Activity on Your System)

- **Sanctions (Required)**
  It is CC policy to appropriately sanction workforce members who violate CC security policies and procedures. A series of escalating sanctions are used. New hires and continuing employees are made aware of these policies through initial training and recurrent annual training. Sanctions for violations of these Security policies and procedures will increase if the violation is serious, intentional and/or repeated. The sanction levels, in order of increasing severity, are as follows:
– Educational reminder - A reminder or explanation of the policy that was violated (Record of Verbal Counseling)
– Verbal Counseling
– Written Counseling
– Suspension of electronic privileges
– Suspension or termination of employment

Management (also the Security Officer) reserves the right to use its discretion in applying sanctions under special or unique circumstances such as but not limited to severity, frequency, and degree of deviation from expectations and length of time involved.

• System Activity Review (Required)
The following policies relate to the regular review of records of activity such as audit logs and access reports in CC Information systems. The purpose of such monitoring is to detect whether anyone is inappropriately accessing or disclosing CC EPHI. CC relies on OIT to monitor the computer system for unauthorized access or use. Any unauthorized use or other evidence of potential data compromise or unauthorized access will be reported to the CC Security Officer. The CC Security Officer, in consultation with OIT and others as needed, will determine what actions, if any, need to be taken to minimize the potential for compromise of EPHI. See also “Security Incident Response and Reporting” in this policy.

Workforce Security Standard
The following policies and procedures are designed to ensure that each staff member has appropriate access to EPHI.

• Authorization and/or Supervision (Addressable)
These policies and procedures are to ensure that users of the CC computer system have appropriate authorization to access EPHI. CC staff members, including clinical staff, administrative staff, and reception staff are authorized to have access to EPHI as needed in the course of performing their responsibilities related to operations, treatment, and record keeping. CC staff supervises other University workforce members or contract vendors (such as repair or maintenance staff, etc) who work near electronic data but who are not authorized to access it.

• Workforce Clearance Procedure (Addressable)
The following policies and procedures apply with respect to prospective (or actual) staff members whose job responsibilities would give them access to, or control over access to, EPHI. Both the CC Security Officer and the UA Human Resources department have policies and procedures for verifying new workforce members’ educational, work and criminal background, reference checks, etc. The CC staff is small and the Security Officer personally orients all new staff to CC security policies and procedures.

• Termination Procedures (Addressable)
When staff members leave CC their access to EPHI is terminated. This includes making sure that the former employee returns keys, ID cards, and timely removal of the staff member from account lists and other access to systems and EPHI. The Security Officer ensures the
staff member’s practice management and electronic medical record user account is inactivated at the time of termination.

Information Access Management Standard
The following policies and procedures pertain to the authorization of access to EPHI.

- **Isolating Health Care Clearinghouse Function (Required)**
  The CC utilizes the services of the Titanium software company for practice management software. The CC has a Business Associate Privacy Agreement with the Titanium software company that outlines CC expectations that the company appropriately protect PHI, including EPHI. In addition, see Transmission Security Standards section of this policy that outlines measures taken to protect EPHI during electronic transmission.

- **Access Authorization (Addressable)**
  These policies and procedures pertain to determining which individuals or entities need to be granted access to EPHI through computers, devices, software, files, transactions, or any other system or mechanism that contains EPHI. Staff members’ access to all computers, devices, software, files, transactions, or any other computer system or mechanism that contains EPHI will be granted based on their role and the application of the policies and procedures listed here for the Workforce Security Standard (Authorization/Supervision and Clearance).

- **Access Establishment and Modification (Addressable)**
  These policies and procedures document the Security Officer's responsibilities in enforcing the policies and procedures that establish access to EPHI. This includes reviewing and modifying a user's access rights to computers, devices, software, files, transactions, or any other computer system or mechanism that contains EPHI, or to modify future access to EPHI when necessary. The Director of CC is responsible for overseeing the process of ensuring only authorized staff members and business associates have access to the computers, devices, software, files, transactions, or any other computer system or mechanisms that contain EPHI, including authorizing access to office keys, network user names and passwords, and/or any other required security access tools as may be required to perform the duties and responsibilities of the staff member or business associate. The Director of CC is responsible for taking appropriate steps to ensure that access is denied to workforce members and business associates who have been terminated or for whom access is no longer appropriate (e.g., return of office keys, deactivating or invalidating unique user names and passwords, and/or recovering or changing any other required security access tools).

Security Awareness and Training Standard
The following policies and procedures ensure that each member of the CC staff is aware of all security policies and procedures that are relevant to his or her job function. All CC employees are trained in security policies and procedures. All employees have access to the policies and procedures manual electronically. The Security Officer will document initial and annual security policies and procedures training.
• **Security Reminders (Addressable)**
The following policies and procedures address keeping staff members apprised of their security responsibilities through reminders:
CC staff are trained on their roles and responsibility relative to this policy as part of new employee orientation, as an annual training requirement, and as needed in staff meetings and via email as well as through other forms of communication. If specific security measures warrant an immediate reminder, one will be sent as necessary via email or other means as appropriate.

**Security Incident Procedures Standard**

• **Response and Reporting (Required)**
The following policies and procedures apply in the event of a "security incident," which is an attempted or actual breach of security (e.g., a hacker breaks into a CC computer, a burglar steals one of the computers, or an unauthorized workforce member looks at EPHI). More precisely, a security incident is an "attempted or successful unauthorized access, use, disclosure, modification or destruction of information." A security incident may also be an attempted or successful interference with an information system (for example, a virus that infects one of the CC computers). Security incidents are reported as soon as possible to the Security Officer. The CC Security Officer, in consultation with OIT and others as needed, will determine what actions, if any, need to be taken to minimize the potential for compromise of EPHI. Law enforcement is notified of a security incident if it is known or suspected to be connected with criminal activity.
  - **Reporting requirements:** Any incidents that come to the attention of any CC/OIT staff member must be reported to the Security Officer or designee as soon as practical, but in no event will it be more than 48 hours after a security incident is discovered or suspected. If the Security Officer is unavailable/out of town, security incidents must be reported to the Security Officer’s delegate. After hours incidents will be monitored and responded to in accordance with the UA Server Registration form on file with IS. The Director of CC can be contacted at any time by calling UAPD at (205) 348-5454 and having dispatch contact the Director of CC.
  - **Personnel/Resources:** CC staff, OIT staff, UAPD staff, and other university resources as appropriate are available to assist in evaluating and responding to real or suspected breaches in electronic security.
  - **Assessment after a security incident** After a security incident is investigated and resolved the Security Officer, in consultation with OIT, the CC Director and others as appropriate, will:
    - Determine whether changes should be made in the CC security policies and procedures to prevent the same type of incident from recurring.
    - Reevaluate existing policies and procedures specifically for responding to a security incident.
    - Document new resources or contacts developed in responding to an incident.

**Contingency Planning Standard**
The following policies and procedures are implemented for the development of a contingency plan to deal with risks that could damage EPHI, e.g., fire, vandalism, system failure, theft, natural disasters.

- **Data Backup Plan (Required)**
  The following policies and procedures ensure that EPHI can be recovered and restored in the event of an emergency, and establish and implement ways to create and maintain retrievable exact copies of all EPHI stored in the Practice’s system. Information Services backs up EPHI on the server daily. Backups of the server occur on a daily basis and are performed as distinct jobs separate from any other jobs run on the backup server. All backup tapes from the CC server are segregated in separate tape pools. These are weekly and monthly tape pools. Tape access is limited to IS personnel and tapes are secured in the UCM Computer Center. On a monthly basis, these tapes are moved to a locked off site storage area for disaster recovery and tape preservation needs. CC maintains paper copies of partial records including when upcoming appointments are scheduled.

- **Disaster Recovery Plan (Required)**
  OIT performs an automatic system back-up on a regular nightly basis. In the event of a catastrophic server failure, CC will work with OIT to restore the practice management data including electronic treatment records, client demographics, and scheduling information from backup to the fullest extent possible. If data is permanently lost or unrecoverable, an entry to the record to that effect will be recorded. CC clinical staff will assess individual patient management situations to determine what clinical information needs to be re-acquired or what assessments need to be repeated in order to ensure continuity of care. In the event that the practice management system and electronic medical record software is unavailable, the CC Director will contact OIT to notify them of the problem with the server. The disaster recovery plan for this possibility includes CC staff maintaining paper copies (e.g., day planners) of their schedules in the event of a system failure. The Titanium software company would send CPS a copy of the practice management software that could be installed on a desk top computer. The most recent back up copy of data from the CC server would be exported into the software. In the event that the scheduling software is unavailable, the receptionist, under the direction and assistance of the CC Director, will reconstruct the schedule by using the individual staff persons’ paper copies and will coordinate client contact and appointment scheduling. Therefore, the CC has created its own Emergency Operations Plan which stipulates that the following critical information must be accessible in the event of an emergency:
  - Client contact information
  - Client mental health records
  - Appointment calendar

- **Emergency Mode Operation Plan (Required)**
  In the event of an emergency, the staff member detecting the emergency will immediately report the emergency to the CC Director. The CC Director is responsible for determining the seriousness of the emergency and initiation of the Emergency Operations Plan, if needed.

- **Applications and Data Criticality Analysis (Addressable)**
The size of the CC does not warrant the creation of a priority listing for computer program recovery.

- **Testing and Revision Procedure (Addressable)**
  The CC will periodically run a test/exercise that consists of the staff reviewing the plan to ensure that everyone knows their roles and responsibilities, and acts in accordance with the policies and procedures, as appropriate and reasonable. To conduct the exercise the CC Director will make a request to OIT. These officials, in cooperation with the Titanium vendor, will plan and schedule the exercise activity. The exercise will include, but not be limited to, a “loss of data” recovery scenario. This exercise scenario will be based on the fact that data has been lost from the server and needs to be recovered. The exercise will include notification to the OIT group that a data loss has occurred along with a request for recovery. This request and notification will occur through a call to the OIT help desk with the request being a “Priority 1” critical need. The Help Desk will create and assign a work order to the appropriate OIT department for action. The OIT department will conduct a restore of a specified static data set and conduct validation tests on the restored data on the server to verify its reliability. This static data set will reside and be protected as if it were true data from the server. This test data will be referred to as the “CC Recovery test data set”.

**Periodic Evaluation Standard**

The following policies and procedures have been enacted to ensure that the CC periodically reassesses its risks and security measures. The CC will conduct a reassessment every year. If the CC has a significant change in its computer systems or personnel structure, the Security Officer will determine whether a security review is necessary prior to the routine reevaluation. To conduct the reevaluation (either routine or because of changes), the Security Officer will reconsider the risk analyses in the electronic record security standards. Changes that need to be made will be documented including the rationale for those changes.

**Business Associate Contract Standard**

The following policies and procedures ensure that the Practice has a Business Associate Contract that appropriately addresses security issues.

- **Written Contract or Other Arrangement (Required)** Business Associate Contracts are in effect with the information management software vendor(s) that provides the CC information management product(s), and OIT personnel who service the CC. These contracts outline the vendor(s) and personnel’s responsibilities to safeguard protected health information, including EPHI.

Policy approval:

_________________________________  ________________
Information Security Officer, OIT     Date

_________________________________  ________________
Counseling Center Director & Security Officer     Date