Insert Your Logo Here

Insert Your Organization Name

Subject: HIPAA Security Policies & Procedures **Policy #: ??-?**

Title: Termination Procedures **Page 1 of 10**

Effective Date of This Revision: June 22, 2017

Contact:	HIPAA Chief Security Officer "Insert Addressee Here" "Insert Street Address Here" "Insert Phone Number Here"	Responsible Department:

HIPAA REGULATORY INFORMATION: Workforce Security Standard

Category:	☒ Administrative Safeguard ☐ Physical Safeguard ☐ Technical Safeguard	**Type:**	☐ Standard ☒ Implementation Specification ☐ Required ☒ Addressable

Applies to:	☒ Officers ☒ Other agents	☒ Staff/ Faculty ☐ Visitors	☒ Student clinicians ☒ Contractors	☒ Volunteers

BACKGROUND:

The Health Insurance Portability and Accountability Act of 1996 *(HIPAA)* requires that access to Protected Health Information (PHI) will be managed to guard the integrity, confidentiality, and availability of electronic PHI *(ePHI)* data. According to the law, all "Covered Entity's Name" officers, employees and agents of units within a "Covered / Hybrid" Entity must preserve the integrity and the confidentiality of individually identifiable health information *(IIHI)* pertaining to each patient or client.

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) [Workforce Clearance Procedure] of this section."

PURPOSE:

Each Unit of "Covered Entity's Name" 's health care component *(HCC)*, which handles ePHI, will have a documented process for terminating access to *ePHI* when the employment of *workforce members* ends or access is no longer appropriate as set forth in "Covered Entity's Name" 's Workforce Clearance Procedure implemented specification ("Policy Number"), Information Access Management standard ("Policy Number") and Access Establishment and Modification implementation specification ("Policy Number"), for example due to a change in position such that the workforce member no longer requires access to *ePHI*.

This policy provides guidance for *"Covered Entity's Name"* 's *Security Office* in adopting the *addressable* Termination Procedure Implementation Specification under the Workforce Security Standard *[C.F.R. 164.308(a)(3)(i)].*

POLICY:

When a "Covered Entity's Name" 's workforce member will be ending their relationship with the covered entity, the affected Human Resources department and the workforce member's supervisor will give reasonable notice to the "Covered Entity's Name" HIPAA Security Compliance Officer, who will then plan the termination of access to the ePHI for the departing workforce member once s/he leaves in accordance with "Covered Entity's Name" 's Access Establishment and Modification policy ("Policy Number") and document all modifications in the Access Authorization Sheet

Each Unit of "Covered Entity's Name" 's (HCC) will log, track, and securely maintain receipts and responses to such termination of access notices, including the following information:

- ☑ Date and time of notice of *workforce member* departure received
- ☑ Date of planned *workforce member* departure
- ☑ Description of access to be terminated
- ☑ Date, time, and description of actions taken

When workforce members end their relationship with "Covered Entity's Name" , all privileges to access ePHI Systems, including both internal and remote information system privileges, will be disabled or removed by the time of departure, or if not feasible, as soon thereafter as possible.

When "Covered Entity's Name" workforce members need to be terminated immediately, "Covered Entity's Name" and/or "Covered Entity's Name" 's HCC will remove or disable their information system privileges before they are notified of the termination, when feasible. Information system privileges include workstations and server access, data access, network access, email accounts, and inclusion on group email lists.

Physical access to areas where ePHI is located will be terminated as appropriate in accordance with "Covered Entity's Name" 's Access Establishment and Modification policy ("Policy Number")"Covered Entity's Name" 's HCC will be alert to situations where workforce members are terminated and may pose risks to the security of ePHI following the Facility Security Plan ("Policy Number").

"Covered Entity's Name" ‘s workforce members will have their ePHI information system privileges disabled after their access methods or user IDs have been inactive for "Number of Days" . "Covered Entity's Name" HIPAA Security Compliance Office will review privileges that are disabled due to inactivity and take the necessary steps to determine the cause of the inactivity. If inactivity is due to termination of employment, "Covered Entity's Name" will promptly terminate all information system privileges and notify appropriate "Covered Entity's Name" personnel to terminate physical access to areas where ePHI is located. If inactivity is due to other causes, "Covered Entity's Name" will complete a review and take measures to terminate, limit, suspend, or maintain the workforce member’s access, as appropriately documented in "Covered Entity's Name" ‘s Access Establishment and Modification policy ("Policy Number")

Each Unit of "Covered Entity's Name" ‘s HCC will ensure that cryptographic keys are recovered and made available to the appropriate managers or administrators if departing workforce members have used cryptography on ePHI.

A workforce member who ends employment with "Covered Entity's Name" will not retain, give away, or remove from "Covered Entity's Name" ‘s premises any ePHI. At the time of his or her departure, a workforce member will provide ePHI in his or her possession to his or her supervisor. "Covered Entity's Name" reserves the right to pursue any and all remedies against workforce members who violate this provision. Departing workforce members’ supervisors will determine the appropriate handling of any ePHI that departing workforce members possess, in accordance with "Covered Entity's Name" ‘s Device and Media Controls policy ("Policy Number").

"Covered Entity's Name" will deactivate or change physical security access codes used to protect ePHI Systems of departing workforce members, when known.

Each Unit of "Covered Entity's Name" ‘s HCC will implement a documented procedure for return of supplied equipment and property that contains or allows access to ePHI, and will disable and remove access to ePHI Systems held by the workforce member, by the time of, or if not feasible, immediately after, the workforce member’s departure.

Each Unit of "Covered Entity's Name" ‘s HCC will track and log the return of equipment and property containing or having the ability to access ePHI with the workforce member’s name, date and time equipment and property was returned, and identification of returned items, and will securely maintain the tracking and logging information on the Inventory tracking sheet. The equipment and property that may contain, or allow or enable the workforce member to access ePHI may include, but is not limited to:

- ☑ Portable computers and Ipads
- ☑ Cellphones/smartphones or other mobile devices
- ☑ Personal Digital Assistants (PDAs)
- ☑ Name tags or name identification badges

- ☑ Security tokens
- ☑ Access Cards
- ☑ Building, desk, or office keys
- ☑ DVD, CD-Rom, Flash Drives etc.

ACTION:

Voluntary Termination (Resignation)

Voluntary termination comes as a result of a workforce member resigning from his/her position. Notice of resignation may be verbal or in writing (preferred).

Steps are as follows:

1. Workforce member notifies "Covered Entity's Name" or supervisor of resignation.
2. "Covered Entity's Name" or supervisor notifies Human Resources within 24 Hours of receipt of resignation. If the workforce member's work location is at a remote location, the notice of resignation will be faxed to Human Resources.
3. "Covered Entity's Name" or supervisor will provide Human Resources with the workforce member's last hours of work to be paid (if a paid position).
4. Human Resources will notify Payroll of termination; pull workforce member's personnel record (if appropriate); and schedule an exit interview with the workforce member (if appropriate).
5. Payroll will produce workforce member's final paycheck within appropriate timeframe and forward to Human Resources for distribution (if a paid position). Payroll will ensure the workforce member receives all pay legally required (e.g. wages, vacation payoff, etc.; if paid position).
6. Human Resources will secure the final paycheck. For workforce members working remotely, Human Resources will forward final pay to workforce member's supervisor or mail directly to the workforce member's home if the workforce member requests.
7. "Covered Entity's Name" or supervisor will notify the security officer or designee and request termination of all access to "Covered Entity's Name" systems and facilities no later than the date of termination, especially remote access to "Covered Entity's Name" network and systems
8. Human Resources will review the workforce member's separation file for completeness and forwards remaining legal notices to workforce member as applicable (e.g., COBRA, 401K, etc.).

Involuntary Termination (Discharge Or Lay-Off):

Involuntary termination/separation may occur under two (2) circumstances: Discharge or Lay-Off. All involuntary terminations are to be reviewed by "Covered Entity's Name", designee or the Human Resources Department prior to taking any action.

Discharge – Discharge normally occurs due to misconduct (breach of company policy or procedure) or substandard work performance. Workforce members terminated for misconduct may not be eligible for rehire. Workforce members terminated for sub-standard work performance may be considered eligible for rehire if the performance-related problem occurs through no direct fault of the workforce member and they have demonstrated a willingness to reapply for another position within the company for which they may be better qualified. In all cases, the decision to rehire a former discharged workforce member remains at the sole discretion of "Covered Entity's Name".

Steps are as follows:

1. Supervisor compiles all documentation to support termination and forwards the documentation to "Covered Entity's Name" or designee prior to taking any action.
2. "Covered Entity's Name" or designee will review the documentation submitted and consults with Human Resources regarding appropriateness and fairness of separation. "Covered Entity's Name" will notify the supervisor of the action to be taken.
3. If discharge is approved, the supervisor will notify Human Resources the workforce member's last working day and total hours worked that pay period (if in a paid position).
4. Human Resources will notify Payroll of termination, pull the workforce member's personnel record (if applicable) and assist the supervisor prepare for involuntary termination.
5. Payroll will produce workforce member's final paycheck within appropriate timeframe and forward to Human Resources for distribution (if a paid position). Payroll will ensure the workforce member receives all pay legally required (e.g. wages, vacation payoff, etc.; if paid position).
6. Human Resources will secure the final paycheck (if a paid position). For workforce members working remotely, Human Resources will forward final pay to the workforce member's supervisor who may be required to travel to workforce member's work location to complete involuntary termination.
7. "Covered Entity's Name" or supervisor will notify the security officer or designee to terminate all access to "Covered Entity's Name" network, systems and facilities no later than the date and prior to the time of the termination, especially remote access to "Covered Entity's Name" computing systems
8. "Covered Entity's Name" or supervisor will meet with the workforce member in private and inform the workforce member the reason for termination. If the workforce member works at a remote location, "Covered Entity's Name" or supervisor will deliver the final paycheck at time of discharge (if a paid position).
9. If the workforce member works at "Covered Entity's Name"'s facility, the supervisor will deliver the final paycheck at time of discharge (if a paid position)
10. Human Resources will reviews the workforce member's separation file for completeness and forwards remaining legal notices to employee (e.g., COBRA, 401k, etc.).
11. If the reason for involuntary discharge is criminal in nature, "Covered Entity's Name" or designee will confer with legal counsel and notify law enforcement and regulatory governmental agencies if appropriate.

***Workforce Reduction (lay off)*:** "Covered Entity's Name" attempts to provide a work environment of growth and job security for its workforce members. However, due to economic or other issues, it may be necessary to reduce the size of the workforce. It is "Covered Entity's Name"'s policy to affect the required workforce reduction in a fair and just manner.

1. Preliminary Measures
   a. Affected workforce members will be encouraged to apply for transfer to other open positions if available.
   b. Paid workforce members may be asked to reduce their scheduled work hours or use accrued paid time off.

2. Permanent Reduction in Force
   a. The identification of affected workforce member(s) will be made by the "Covered Entity's Name", designee and, if applicable, reviewed by Human Resources.
   b. The decision regarding which workforce members are affected shall be based on a combination of factors, including but not limited to:
      i. Requirements of "Covered Entity's Name" operations
      ii. Documented qualifications to perform the work required
      iii. Documented performance levels
      iv. Documented counseling
      v. Seniority in "Covered Entity's Name" organization, based on actual hire date.
   c. Workforce members affected will be terminated from the active payroll and have no recall rights [*"Covered Entity's Name" needs to take into account union or other contracts that may impact the "no recall rights" clause*]. However, they may apply for any open position for which they are qualified, and may be considered for re-employment as any other applicant. "Covered Entity's Name" or "Covered Entity's Name" management retains the right to offer any available job to the candidate who is best qualified based on skills, experience and education.
   d. Affected workforce members will receive all benefits as upon any termination, such as payout of all accrued paid time off and COBRA continuation of benefits (if a paid position).
   e. Severance Pay may be available to the affected workforce members. Severance Pay is designed to assist affected workforce members in their transition, according to the following guidelines:
      i. Eligibility for Severance Pay is limited to regularly scheduled full-time and part-time employees. Temporary or volunteer staff are not eligible for Severance Pay. Contracted staff are governed by their specific contract.
      ii. The amount of Severance Pay is based on [*"Covered Entity's Name" severance pay basis, if any*].
      iii. Severance Pay will be paid in one lump sum with all deductions, on the last day of employment, along with accrued paid time off, if any.
      iv. If the affected employee refuses an offer of another position within the "Covered Entity's Name" organization which is paid within 10% of his/her current base rate, and is located within a reasonable distance from the current job, Severance Pay will be denied.

v. If the affected employee returns to regular employment within one month of the original reduction in workforce, he/she may retain all prior seniority and benefits only if all Severance pay is returned at the time of rehire.

vi. Employees may voluntarily elect to be eliminated from the workforce to save another co-worker's job, and will receive Severance Pay if otherwise eligible. However, "Covered Entity's Name" reserves the right to refuse such offers based on "Covered Entity's Name"'s needs.

vii. As with all policies, "Covered Entity's Name" may modify, change, or eliminate this policy at any time, with or without notice.

Steps are as follows:

1. "Covered Entity's Name" or supervisor will consult with appropriate senior management and Human Resources immediately when a workforce reduction is anticipated.
2. "Covered Entity's Name" or supervisor will identify affected workforce members and validate with Human Resources to ensure compliance with the Workforce Reduction Policy.
3. Human Resources will determine whether notice or Severance Pay is appropriate.
4. "Covered Entity's Name" or supervisor will meet with affected workforce member and provide them written notice of intent to lay-off and will provide as much notice as possible to all affected workforce members.
5. "Covered Entity's Name" or supervisor will meets with remaining workforce members if appropriate and explains lay-off procedure and future effect.
6. On the day before the effective date of the lay-off, "Covered Entity's Name" or supervisor will forward to Human Resources the workforce member's last working day and total hours worked that pay period (if in a paid position).
7. Payroll will produce workforce member's final paycheck within appropriate timeframe and forward to Human Resources for distribution (if a paid position). Payroll will ensure the workforce member receives all pay legally required (e.g. wages, vacation payoff, etc.; if paid position).
8. Human Resources will secure the final paycheck (if a paid position). For workforce members working remotely, Human Resources will forward final pay to the workforce member's supervisor or to the workforce member's home, if requested by the workforce member.
9. "Covered Entity's Name" or supervisor will meet with workforce member(s) on the workforce member'(s) last day and individually communicate with all impacted workforce members and distribute final paychecks (if a paid position).
10. "Covered Entity's Name" or supervisor will notify the security officer or designee to terminate all access to "Covered Entity's Name" network, systems and facilities no later than the date of termination, especially remote access to "Covered Entity's Name" computing systems.
11. Human Resources will distribute final paychecks and conducts exit Interviews, if appropriate.

Involuntary or Voluntary Termination of Relationship with Third Party Affiliates:

Relationship termination of a relationship with a third party affiliate may occur because of contract or affiliation termination/non-renewal, joint agreement to terminate affiliation or because of misconduct on

the part of the third party affiliate. Under all circumstances, termination to "Covered Entity's Name" network, systems and facilities is required upon termination of the relationship.

Steps are as follows:

1. "Covered Entity's Name" will discuss with legal counsel any involuntary termination of affiliation with a third party to determine what steps are necessary such as notice in advance, contract termination, etc.
2. Following consultation with legal counsel, "Covered Entity's Name" will notify affiliated third party of the termination of the relationship and the reason for termination.
3. The affiliated third party may also sever the relationship with "Covered Entity's Name" with notice to "Covered Entity's Name", taking account of legal requirements related to any contractually agreements that may have been entered into between "Covered Entity's Name" and affiliated third party.
4. "Covered Entity's Name" or supervisor will notify the security officer or designee to terminate all access to "Covered Entity's Name" network, systems and facilities no later than the date of relationship termination, especially remote access to "Covered Entity's Name" computing systems.
5. "Covered Entity's Name" will require the return of any portable devices, media or other hardware or software that is the property of the "Covered Entity's Name" from the affiliated third party and take necessary legal steps if affiliated third party refuses to return "Covered Entity's Name" assets/ property.
6. If termination of the relationship is involuntary due to misconduct/violation of "Covered Entity's Name"'s privacy and security standards, the security officer or designee will terminate access on the date of termination but prior to the time of termination, especially to remote systems.
7. If the reason for involuntary relationship termination is criminal in nature, "Covered Entity's Name" or designee will confer with legal counsel and notify law enforcement and regulatory governmental agencies if appropriate.

DEFINITIONS:

HIPAA: Health Insurance Portability and Accountability Act of 1996

Electronic Protected Health Information (ePHI): Electronic health information or health care payment information, including demographic information collected from an individual, which identifies the individual or can be used to identify the individual. ePHI does not include students records held by educational institutions or employment records held by employers, or records for persons deceased for over 50 years.

Individually Identifiable Health Information (IIHI): Information that is a subset of health information, including genetic information and demographic information collected from an individual, and:

- ☑ Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
- ☑ Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
- ☑ That identifies the individual; or
- ☑ With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

"Covered Entity's Name" Health Care Component (HCC): Those units of "Covered Entity's Name" that have been designated by the "Covered Entity's Name" as part of its health care component under HIPAA.

"Covered Entity's Name" Security Officer: the individual appointed by "Covered Entity's Name" to be the HIPAA Security Officer under s. 164.306(2) of the HIPAA Security Rule.

Addressable: When a standard adopted under 45 CFR Part 164.312 includes addressable implementation specifications, a unit within the "Covered Entity's Name" HCC must (i) assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting the unit's electronic ePHI and (ii) as applicable to the unit: (A) implement the implementation specification if reasonable and appropriate; or (B) if implementing the implementation specification is not reasonable and appropriate: (1) document why it would not be reasonable and appropriate to implement the implementation specification; and (2) implement an equivalent alternative measure if reasonable and appropriate.

Related Policies:

Access Establishment and Modification ("Policy Number")

"Covered Entity's Name" Confidentiality Agreement

Information Access Management Standard ("Policy Number")

Workforce Clearance ("Policy Number")

Reference:

Access to Electronic Health Information Flow Sheet

Access Authorization ("Policy Number")

"Covered Entity's Name" Confidentiality Agreement

HIPAA Final Security Rule, 45 CFR Parts 160, 162, and 164, Department of Health and Human Services, http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp, February 20, 2003.

HIPAA Omnibus Rule, revisions to 45 CFR Parts 160, and 164, Department of Health and Human Services, http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf, January 25, 2013.

CMS, “CMS Information Systems Security Policy, Standards and Guidelines Handbook”, CMS, February 2002.

International Standards Organization (ISO/IEC 17799:2000(E))

National Institute of Standards and Technology (NIST) Special Publication 800-66 Rev. 1, An Introductory Resource Guide for Implementing the HIPAA Security Rule, http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf.