COUNTY OF LOS ANGELES **DEPARTMENT OF HEALTH SERVICES**

HARBOR-UCLA MEDICAL CENTER

POLICY: SUSPECTED MISUSE OF PROTECTED HEALTH INFORMATION BY A WORKFORCE MEMBER **POLICY NO. 751**

PURPOSE:
To establish guidelines for reporting suspected misuse of Protected Health Information (PHI) by Harbor-UCLA Medical Center's workforce members, including contractors and volunteers.

POLICY:
Harbor-UCLA Medical Center's workforce members, including contractors and volunteers, must immediately report any suspected misuse of PHI.

PROCEDURE:
If a Harbor workforce member, contractor, or volunteer (hereafter referred to collectively as "employee") is suspected of misuse of PHI, the following actions shall be taken:

A. Supervisor

The Supervisor shall immediately:

1. Identify if the misuse is a HIPAA privacy issue, security issue, or both;
2. Identify what access – if any – the employee has to electronic PHI (i.e., Electronic Health Record, Leader, Casewatch, MIDAS, medical department-specific data systems, etc.);
3. Notify in writing the Department Chair/Service Director of his/her department of the suspected PHI misuse, and what access, if any, the employee has to electronic PHI.
   Note: If the suspected misuse needs to be addressed immediately, direct verbal notification (not by voice mail) is acceptable for initial notification. Written notification should be made as soon as possible thereafter.
4. Submit a Safety Intelligence (SI) report to document the suspected PHI misuse.
5. Develop a chronology of events related to this matter.

B. Department Chair/Service Director/Nurse Manager

The Department Chair/Service Director/Nurse Manager shall:

1. Notify the appropriate HIPAA Coordinator of the suspected PHI misuse, and jointly determine whether to temporarily suspend the employee's access to electronic PHI systems. Notify the Facility Privacy Manager at ext. 6575 if the suspected misuse involves privacy issues; notify the Facility Security Officer at ext. 2181 if it involves security issues.
   a. If the decision is made to temporarily suspend such access, the Department Chair/Service Director shall reassign the employee to non-PHI related duties.

EFFECTIVE DATE: 06/07 **SUPERSEDES:**
REVISED: 2/18
REVIEWED: 2/15, 2/18
REVIEWED COMMITTEE:

APPROVED BY:

Kim McKenzie, RN, MSN, CPHQ
Chief Executive Officer

Anish Mahajan, MD
Chief Medical Officer

Patricia Soltero Sanchez, RN, BSN, MAOM
Chief Nursing Officer

Signature(s) on File.

2. Notify Hospital Administrator (designee) at ext. 2101 of the suspected misuse. After-hours, notify the Administrator of the Day by pager (310) 233-5245.
3. Notify Human Resources at ext. 3241 of the suspected PHI misuse, and report any actions to temporarily suspend the employee's PHI access and/or reassign the employee to non-PHI related duties. Jointly determine if administrative or disciplinary actions -- including administrative leave or suspension -- should be taken, and what those actions should be.
4. Implement and document the remediation recommendations.
5. Report in writing, completion of the recommendations to the HIPAA Security Officer and/or HIPAA Privacy Manager. Forward all relevant documentation of the remediation.

C. Human Resources Director (Designee)

The Human Resources Director (designee) shall:

1. Work with the Department Chair/Service Director/Nurse Manager to:
   a. Review decisions to temporarily suspend the employee's PHI access.
   b. Jointly determine the appropriateness and necessity of initiating administrative or disciplinary actions -- including paid and/or unpaid administrative leave or suspension -- and what those actions should be.
2. Initiate and document agreed-upon administrative and/or disciplinary actions.
3. Report initiation of administrative and/or disciplinary actions to the:
   a. Facility Privacy Manager, if the suspected misuse involves HIPAA privacy issues.
   b. Facility Security Officer, if the suspected misuse involves HIPAA security issues.

D. HIPAA Privacy Coordinator

1. If the suspected misuse involves HIPAA privacy issues, the HIPAA Privacy Coordinator shall:
   a. Report the suspected PHI misuse and follow-up actions to the DHS Privacy Officer within 24 hours of filing the report or sooner.
   b. Notify the HIPAA Security Coordinator.
   c. Verify what access – if any -- the employee has to electronic PHI systems.
   d. Determine – in consultation with the employee's Department Chair/Service Director/Nurse Manager -- whether to temporarily suspend the employee's access to electronic PHI systems.

      If the decision is made to temporarily suspend such access, the HIPAA Privacy Coordinator shall:
      - Notify the Department Chair/Service Director, so that manager can make necessary workforce adjustments.
      - Instruct the Director of Information Systems Services and the Director of Information Technology (or their designees) to de-activate the employee's access to all electronic PHI systems. **Note:** After hours, contact the IT Help Desk at ext. 5059.
   e. Report suspected PHI misuse to:
      - DHS Audit & Compliance Office at (213) 240-7901.
      - DHS Privacy Officer at (213) 240-7741.
   f. Initiate with the HIPAA Security Coordinator an investigation of the suspected PHI misuse.

g. Identify appropriate remediation recommendations (including timelines); submit those recommendations in writing to the Department Chair/Service Director/Chief Information Officer/Hospital Administrator.

E. HIPAA Security Coordinator

1. If the suspected misuse involves HIPAA security issues, the HIPAA Security Coordinator shall:
   a. Verify what access – if any -- the employee has to electronic PHI systems.
   b. Determine – in consultation with the employee's Department Chair/Service Director/Nurse Manager -- whether to temporarily suspend the employee's access to electronic PHI systems.

      If the decision is made to temporarily suspend such access, the HIPAA Security Coordinator shall:
      - Notify the Department Chair/Service Director, so that manager can make necessary workforce adjustments.
      - Instruct the Director of Information Systems Services and the Director of Information Technology (or their designees) to de-activate the employee's access to all electronic PHI systems. **Note:** After hours, contact the IT Help Desk at ext. 5059.

   c. Report suspected PHI misuse to:
      - DHS Audit & Compliance Office at (213) 240-7901.
      - DHS Privacy Officer at (213) 240-7741.
   d. Initiate with the HIPAA Privacy Coordinator an investigation of the suspected PHI misuse.
   e. Identify appropriate remediation recommendations (including timelines); submit those recommendations in writing to the Department Chair/Service Director/Chief Information Officer/Hospital Administrator.