COUNTY OF LOS ANGELES

PROBATION DEPARTMENT

DIRECTIVE

No.: Revised 1384
Issued: 08/05/15
Post until: 09/05/15

SUBJECT: RESPONDING TO BREACHES OF PERSONALLY IDENTIFIABLE INFORMATION (PII) AND PROTECTED HEALTH INFORMATION (PHI)

The purpose of this Directive is to establish a policy and procedures for the Probation Department's workforce members to adhere to in the event a breach or suspected breach of PII or PHI is discovered.

Policy

It is the Probation Department's policy to investigate and notify the County's Chief Information Security Officer (CISO) and Chief HIPAA Privacy Officer (CHPO) immediately (same business day) upon discovery of a breach of unsecured PII or PHI.

Definitions

- **Breach** – The term breach refers to the unauthorized acquisition, access, use, or disclosure of PII and/or PHI which compromises the security, privacy, or integrity of such information.
- **Personally Identifiable Information (PII)** – PII is any information maintained by the Department that identifies or describes an individual, including, but not limited to, name, Social Security Number (SSN), date of birth, physical description, home address, telephone number, education, financial matters, medical, or employment history. PII applies to all Bureaus.
- **Protected Health Information (PHI)** – PHI is any information maintained, created, or received by the Department that relates to the past, present, or future health, or payment for health care that is individually identifiable health information, such as a person's name or SSN that is transmitted or maintained in any form or medium, including electronic information, written, or verbal. An example of PHI is any patient information maintained, used, or disclosed by a covered department to Probation, such as patient's name, medical record number, financial information, diagnosis, address, treatment, payment history, etc. Currently, PHI is accessible through and stored within the Probation Electronic Medical Records System (PEMRS).
- **Unsecured PII or PHI** – Unsecured PII or PHI is any PII or PHI that is not rendered or determined by the CISO or CHPO to be unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology (e.g., encryption).
- **Discovered** – A breach of PII or PHI will be deemed discovered as of the first day a Department workforce member knows of the breach, or by exercising reasonable diligence, would or should have known about the breach.

Procedures

1. If a workforce member discovers or becomes aware of a breach or suspected breach of PII or PHI, he or she must immediately (same business day) report the incident to his or her Bureau Chief, who shall ensure that the breach is reported to the Probation Department Information Security Officer (DISO) and CHPO.

2. If the breach involves PII, the Probation DISO shall make the initial report by telephone call to (562) 940-3335 immediately when he or she becomes aware of the breach, followed by a full written report to the CISO at CISONotify@cio.lacounty.gov no later than 10 business days from the date he or she becomes aware of the breach.

3. If the breach involves PHI, the Bureau Chief shall ensure that the initial report is made by telephone call to (213) 974-2164, which is the HIPAA Hotline, or e-mail at HIPAA@auditor.lacounty.gov. The Bureau Chief, or his or her designee, will work with the CHPO in producing a full written report no later than 10 business days from the date the breach was reported to the CHPO.

4. Following the initial notice of the discovery of a breach, the Probation Department, CISO, and CHPO shall conduct a risk assessment to determine if the breach is an unsecured or secured breach of PII or PHI, and exercise any mitigation efforts to prevent the breach from occurring again.

Note to workforce members: Employment records are excluded from the definition of PHI, see 45 C.F.R. § 164.103. In other words, employment records are not under the jurisdiction of the HIPAA regulations. For disclosures of PHI made for Workers' Compensation purposes under 45 CFR 164.512(l), HIPAA permits disclosures of information to the full extent authorized by the State or other laws.

Authority

45 C.F.R. §164.504; Section 13402 of Title XIII, Health Information Technology for Economic and Clinical Health Act of the American Recovery and Reinvestment Act of 2009; AB-1149 Identity Theft: Civil Code §1798.29; Board of Supervisors Policy 6.109; and Board of Supervisors Policy 3.040.

For any questions or concerns regarding this Directive, please contact the Probation DISO at (562) 940-2843.

Jerry E. Powers, Chief Probation Officer

Attachment(s): Report #2008-001 - Computer Security Incident Report
Form - Reporting an Unsecured PHI Breach to the CHPO

Countywide Information Security Program

PROBATION

Report #	Computer Security Incident Report	Date
2008 - 001		mm / dd / yyyy

In accordance with County policy # 6.109 Security Incident Reporting, a report must be filed with the County's Chief Information Security Officer (CISO) when an IT related security incident occurs. The completed report may be emailed to CISOnotify@cio.lacounty.gov. The report must delineate the scope of the incident, impact, action(s) being taken and any action(s) taken to prevent a further occurrence.

Type of Incident
(Incident types are: Stolen/Lost, Intrusion/Hack, Web Defacement, System Misuse, Denial of Service, Spoofed IP Address, Unauthorized Probe/Scan, Unauthorized Electronic Monitoring, Malicious Code (virus, worm, etc.), and other.)

Date and Time when Incident was Identified / Discovered

Location of Incident
(Physical address including specific building location)

Who Identified / Reported the Incident
(Full Name, Job Title / Position, email address, and Phone number (e.g., work, cell, etc.))

Workforce Members Involved with the Incident and/or with the Response
(Full Name, Job Title / Position, email address, and Phone number (e.g., work, cell, etc.))

Brief Synopsis by the Departmental Information Security Officer (DISO)
(Narrative or chronology)

Date and Time of the Incident (If known)

Department Initial Response

Action(s) Taken to Prevent Further Occurrence

Action(s) Planned to Prevent Further Occurrence

Internal Services Department Service Center and/or Departmental Problem Ticket(s) #
(Countywide Computer Security Incident Hot-Line number is (562) 940-3335)

Was Personally Identifiable Information (Pii) (i.e., Confidential / Sensitive) involved?

☐ Yes ☐ No ☐ Unknown

Was the device / information encrypted?

☐ Yes ☐ No ☐ Unknown

Was a Law Enforcement Report taken?

☐ Yes ☐ No ☐ Unknown Agency _____ Report # _____

Departmental Information Security Officer – Print Name (First and Last), Sign, Date & Time

Departmental Information Technology Manager (or designee) – Print Name (First & Last), Sign, Date & Time

Departmental Chief Information Officer (or designee) – Print Name (First and Last), Sign, Date & Time

CISO (or designee) – Print Name (First and Last), Sign, Date & Time **(signature signifies receipt)**

County of Los Angeles
DEPARTMENT OF PROBATION
INFORMATION TECHNOLOGY SECURITY COMPUTER INCIDENT REPORT

In accordance with Board approved County-wide security Policy # 6.109, Security Incident Reporting, an incident report must be filed by the next business day with the County's Chief Information Security Officer when a computer related security incident occurs. The report must delineate the scope of the computer incident, impact, action(s) being taken and any action(s) taken to prevent a further occurrence.

In order to comply with this requirement, Probation Management, e.g., district/region Office Head, or a designee, must use this seven part form to report a computer related incident to the Department's Information Security Officer (DISO) or Information System Bureau's CIO by the next business day after the occurrence. The reporting should be done as follows:

- Contact the Information Systems Bureau Help Desk by phone at

  (866) 607-3171

  to report the incident or the DISO by the next business day

- Complete the written report
- Immediately send a copy of the completed report via e-mail to the DISO
- Continue providing updates (if any) as they arise by e-mail or by telephone to the DISO
- Mail the original report to the DISO at Downey Headquarters

Part V of this report is to be completed by IT Network/Technical staff when a security incident has affected the network.

In the event of stolen property, the Office Head will determine if local police should be contacted. However, escalation of the incident outside of the Department is the responsibility of the DISO.

NOTE:

This report <u>does not replace</u> the CEO's Office of Security Management Security Incident Report (SIR). It is to be completed in addition to the SIR.

Board approved and departmental security policies are available through the "Information Technology Security" link on our Probnet home page.

County of Los Angeles

DEPARTMENT OF PROBATION

INFORMATION TECHNOLOGY SECURITY COMPUTER INCIDENT REPORT

(This report is to be used for incidents related to technology)

PART I - Contact Information-Mandatory

Facility Name (where incident occurred):	Department or Division Location:	
Contact name:	Phone #:	E-mail address:

PART II - Incident Information-Mandatory

Date incident occurred:	Date incident discovered:	Employee/participant safety affected? Yes ☐ No ☐	Location of Incident:
Time incident occurred:	Time incident discovered:	Incident Affects What Services? N/A ☐	How many PCs/files and/or records affected? N/A ☐

PART III - Describe Type of Incident-Mandatory (please use additional sheets if necessary) or check N/A (Not Applicable)

System Compromise/Intrusion (check one): NA ☐
Root Compromise ☐ User Compromise ☐
Loss, Theft, or Missing (check one): NA
Desktop ☐ Laptop ☐ Media ☐
Other (please specify)_____
Malicious Code (check one): NA
Trojan ☐ Virus ☐ Worm ☐

(Check one): N/A ☐
Web Site Defacement ☐
Denial of Service ☐
Critical Infrastructure ☐
Protection ☐
Unauthorized Use ☐

Information Compromise ☐
Attempted Intrusion ☐
Reconnaissance Activity ☐
Stolen Equipment ☐
Other (please specify

PART IV - Detail on Information Security-Mandatory (please use additional sheets if necessary) or check N/A (Not Applicable)

Information sensitivity (check one):	Security Category (check one):	Description of how information was stored/ contained/ packaged (i.e., password, encrypted, locked briefcase, etc.):
Personal Identifiable Information (PII) ☐ No Personal Identifiable Information ☐ Other (please specify)_____	Low Security: *limited* adverse affect ☐ Moderate Security: *serious* adverse affect ☐ High Security: *severe/catastrophic* adverse effect ☐	
Which critical infrastructure was affected, if any? N/A ☐		Is network traffic affected? Yes ☐ No N/A ☐ (If yes, IT network/technical staff competes Part V)

PART V - IT Network/Technical Security, if appropriate (please use additional sheets if necessary) or check N/A (Not Applicable)

IP address of affected equipment(s): N/A ☐	Domain name of affected equipment(s): N/A ☐
Operating system(s) of affected equipment(s): N/A ☐	Last time the affected equipment(s) patched : N/A ☐
Functions of affected equipment(s): N/A ☐	Application software affected: N/A ☐

Description of incident:	Destination Port(s) and Protocol(s): N/A ☐
Method of detection:	Country(ies) of attacker(s): N/A ☐
What security infrastructure was in place:	
IP address(es) of attackers: N/A ☐	Domain name(s) of attacker(s): N/A ☐
Suspected method of intrusion/attack: N/A ☐	
Suspected violator and/or possible motivations:	
Name of Trojan(s) or malicious code(s): N/A ☐	Evidence of spoofing: N/A ☐

PART VI - Impact and Actions Taken (please use additional sheets if necessary)

What physical security was in place:	
Assessment of the impact of the incident (include sequence of events):	News Media Activity/Attention? Yes ☐ No ☐
Is this incident affecting Services? Yes ☐ No ☐	Is this a recurring event? Yes ☐ No ☐
What actions have been taken/resolution:	
Were you contacted by an outside agency? Yes ☐ No ☐ If yes, give agency contact information:	
Could this incident escalate to any Official Office (i.e., Dept. Head, Board of Supervisors, Congress Rep., etc)? Yes ☐ No ☐	

Who has been notified? Departmental Information Security Officer ☐ Other Sections/Agencies involved/notified (please specify)	Incident Report to: ISB Helpdesk Ticket #___ ISD Helpdesk Ticket #___ Police (attach copy) Report #
Other information:	If PII is involved, have affected people been notified? Yes ☐ No ☐

PART VII - Report Information

Report Date:	Reporting Office:	Reporter's Phone Number:
Print Reporter Name & Title:		Reporter's Signature:
Print Office Head/Designee Name & Title:		Office Head/designee Signature:

Management (district/region Office Head, or designee), must report the incident by the next business day after its occurrence to the Department's Information Security Officer or ISB's CIO. Please continue to report any updates (if any) as they arise by e-mail or by telephone to the DISO.

ATTACHMENT A

Form for Reporting an Unsecured Protected Health Information Breach to the Chief HIPAA Privacy Officer, Department of Auditor-Controller

Covered Department/Business Associate:

Department/Business Associate: _____
Contact Name: _____
Address: _____
Contact Phone: _____
E-mail Address: _____

Breach Affecting:

☐ 500 or More Individuals: (Date reported to CHPO_____)

☐ Less Than 500 Individuals

Number of individuals impacted is _____

Breach Start Date: _____ **Breach End Date:** _____

Discovery Start Date: _____ **Discovery End Date:** _____

Type of Breach: Please select the type of breach from one of the following categories.

☐ Hacking/IT Incident

☐ Improper Disposal

☐ Loss

☐ Theft

☐ Unauthorized Access/Disclosure

Location of Breach Information: Please select the location of the information at the time of the breach. If selecting the "Other" category, please describe the location of the information in more detail in the Description section below.

☐ Desktop Computer

☐ Electronic Medical Record

☐ Email

☐ Laptop

☐ Network Server

☐ Other Portable Electronic Device

☐ Paper/films

☐ Other

Describe Other:

Type of Protected Health Information Involved in the Breach: Please select the type of protected health information involved in the breach. If selecting an "Other" category, please describe the information in detail below.

Clinical Information: if yes, check those that apply:

☐ Diagnosis/Conditions

☐ Lab Results

☐ Medications

☐ Other Treatment Information

Demographic Information: if yes, check those that apply:

☐ Address/Zip

☐ Date of Birth

☐ Driver's License

☐ Name

☐ SSN

☐ Other Identifier

Financial Information: if yes, check those that apply:

☐ Claim Information

☐ Credit Card/Bank Account No.

☐ Other Financial Information

Describe other:

Brief Description of the Breach: Please include the location of the breach, a description of how the breach occurred, and any additional information regarding the type of breach, type of media, and type of protected health information involved in the breach.

Safeguards in Place Prior to Breach: Please indicate what protective measures were in place prior to the breach.

☐ None

☐ Privacy Rule Safeguards (Training, Policies and Procedures, etc.)

☐ Security Rule Administrative Safeguards (Risk Analysis, Risk Management, etc.)

☐ Security Rule Physical Safeguards (Facility Access Controls, Workstation Security, etc.)

☐ Security Rule Technical Safeguards (Access Controls, Transmission Security, etc.)

Was Individual(s) Notified of the Breach?

☐ Yes ☐ No

Individual Notice Provided State Date: _____
Individual Notice Provided End Date: _____

Was Substitute Notice Required?

☐ Yes ☐ No

Was Media Notice Required with this Breach?

☐ Yes ☐ No

Actions Taken in Response to Breach: Please select the actions taken to respond to the breach. If selecting the "Other" category, please describe the action taken in the section below.

☐ Adopted encryption technologies

☐ Changed password/strengthened password requirements

☐ Created a new/updated Security Rule Risk Management Plan

☐ Implemented new technical safeguards

☐ Implemented periodic technical and nontechnical evaluations

☐ Improved physical security

☐ Performed a new/updated Security Rule Risk Analysis

☐ Provided business associate with additional training on HIPAA requirements

☐ Provided individuals with free credit monitoring

☐ Revised business associate contracts

☐ Revised policies and procedures

☐ Sanctioned workforce members involved (including termination)

☐ Took steps to mitigate harm

☐ Trained or retrained workforce members

☐ Other

Describe other actions taken:

Please submit the above to:

Department of Auditor-Controller, HIPAA Compliance Unit
Kenneth Hahn Hall of Administration
500 West Temple Street, Room 410
Los Angeles, California 90012
E-mail: ltmcbride@auditor.lacounty.gov and jchen@auditor.lacounty.gov