			Reporting Security Incidents Involving Paper, Electronic Records, or Other Formats by Service Providers & Vendors
			POLICY
Document No. **N/A**	**Version No.** **1** **9/18/17**	**Effective Date** **07/1/2017**	**Author: Chief Financial Officer's Office**

1. PURPOSE

The purpose of this Policy and Procedure is to establish guidelines on the reporting of security incidents, involving paper, electronic records, and other formats, when there has been a breach of personal identifying information by any of NLACRC's service providers or vendors.

2. APPLICABILITY

This policy and procedure affects all service providers or vendors that have access to confidential Protected Health Information ("PHI") or Electronic Protected Health Information ("EPHI").

3. POLICY DETAIL

It is the Policy of NLACRC to protect the privacy and security of PHI and EPHI as stipulated by the Health Insurance Portability and Accountability Act ("HIPAA"); and in accordance with NLACRC's contract with Department of Developmental Services ("DDS"), and DDS's Community Operations Division ("COD") Program Advisories.

The purpose of this policy is to establish the guidelines for the reporting of security incidents by NLACRC service providers and vendors when PHI or EPHI has been breached.

4. APPLICABLE PROCESSES

4.1 All service providers and vendors who have access to PHI or EPHI shall execute a business associate agreement with NLACRC, which requires the service provider or vendor to immediately notify NLACRC of any security breach of PHI or EPHI.

4.2 The "Reporting Security Incidents, Involving Paper, Electronic Records, or Other Formats, for Service Providers and Vendors" Policy shall be posted on NLACRC's website at www.nlacrc.org.

4.3 Any loss or theft of personal, sensitive, or confidential information in any format, collected and stored by the service provider or vendor, shall be reported, within one (1) business day, to NLACRC's Privacy Officer, or their designee, at privacyofficer@nlacrc.org.

4.4 The Privacy Officer, or their designee, shall require the service provider or vendor to complete the following information within one (1) business day.

4.4.1 Information Security Incident Report (SIMM 5340-B)
4.4.2 Copies of Notification Letters to Consumers and Families
4.4.3 Police report, if applicable

4.5 The NLACRC Privacy Officer, or their designee, shall submit the completed SIMM 5340-B Form, copies of notification letters to consumers and families, and police report, if applicable, to DDS at iso@dds.ca.gov within one (1) business days of the NLACRC's receipt of the information from the service provider or vendor.

4.6 Any notification of a security breach by a service provider or vendor may require an internal review and assessment of the incident and of the service provider's or vendor's business practices to determine if changes are needed to prevent future occurrences and to mitigate future risks.

4.6.1 Under the direction of the Privacy Officer, or their designee, this internal review may involve representatives to include, but are not limited to Department of Developmental Services, Administration, Case Management, Community Services, and Clinical Department.

5. REFERENCES/FORMS

5.1 Business Associate Agreement is published on NLACRC's website. The hyperlink to the Agreement is https://www.nlacrc.org/modules/showdocument.aspx?documentid=3489

5.2 Information Security Incident Report (SIMM 5340-B), September 2013

5.3 Sample "Notice of Data Breach" Letter

5.4 DDS Community Operations Division ("COD") Program Advisory, COD 09-01

6. DEFINITIONS

6.1 "Breach" shall mean the unlawful or unauthorized access to, viewing, acquisition, use or disclosure of PHI or EPHI.

6.2 "HIPAA" shall mean the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, title X111 of the American Recovery and Reinvestment Act of 2009, Public Law 111-005, and

regulations promulgated thereunder by the U.S. Department of Health & Human Services, as amended from time to time.

6.3 "Protected Health Information" ("PHI") shall have the meaning given to such term under HIPAA and shall include any information, whether oral or recorded in any form or medium, limited to the information created or received by Subcontractor from or on behalf of Business Associate (i) that relates to the past, present or future physical or mental health condition of the Consumer; the provision of health care to Consumer; or the past, present or future payment for the provision of health care to Consumer; and (ii) that identifies the Consumer or with respect to which there is a reasonable basis to believe the information can be used to identify the Consumer.

6.4 "Service Provider" refers to any individual, partnership, group association, corporation, institution, independent contractor, or entity which has been given a vendor identification number and has completed the vendorization process; pursuant to Welfare and Institutions Code ("WIC") section 4648 (a)(3).

6.5 "Subcontractor" shall have the same meaning given such term under HIPAA, and includes a person to whom a Business Associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.

6.6 "Vendor" refers to any individual, partnership, corporation, institution, independent contractor, or entity that performs functions for or on behalf of NLACRC and has access to protected health information in the performance of its functions.

State of California

California Information Security Office

Information Security Incident Report

SIMM 5340-B

(formerly SIMM 65C)

September 2013

REVISION HISTORY

REVISION	DATE OF RELEASE	OWNER	SUMMARY OF CHANGES
Initial Release	**August 2012**	**California Office of Information Security**	
Minor Update	**September 2013**	**California Information Security Office**	**SIMM number change, change "agency" to "state entity"**

State Entity Name: _____

State Entity Organization Code: _____

(As identified in the Uniform Codes Manual)

Incident Number: _____

(Provided by the California Information Security Office)

A. Notification

1. Date of notification to the California Highway Patrol (CHP) Emergency Notification and Tactical Alert Center (ENTAC): _____

B. Incident Information

1. Details of Incident:

a) Date incident occurred: _____ ☐ Unknown

b) Date incident detected: _____ ☐ Unknown

c) Incident location: _____

d) General description:

_____

e) Media/Device type, if applicable: _____

Was the portable storage device encrypted? ☐ Yes ☐ No

If NO, explain: _____

f) Describe the costs associated with resolving this incident:

_____

g) Total estimated cost of incident: _____

2. Incidents involving personally identifiable information

a) Was personally identifiable information involved? ☐ Yes ☐ No (If No, go to Part C)

Type of personally identifiable information (Check all that apply)

☐ Name
☐ Health or Medical Information
☐ Social Security Number
☐ Financial Account Number
☐ Driver's License/State ID Number
☐ Other (Specify) _____

b) Is a privacy disclosure notice required? ☐ Yes ☐ No

c) If a Privacy Disclosure Notice is required, attach a sample of the notification.

d) Number of individuals affected: _____

e) Date notification(s) made: _____

C. Corrective Actions Planned/Taken to Prevent Future Occurrences:

_____

1. Estimated cost of corrective actions: _____

2. Date corrective actions will be fully implemented: _____

D. Signatures:

Printed Name of Information Security Officer	Signature of Information Security Officer	(Date)
Printed Name of Privacy Officer *(Required if privacy incident occurred whether or not notices were sent)*	Signature of Privacy Officer	(Date)
Printed Name of Secretary/Director or Designee	Signature of Secretary/Director or Designee	(Date)

Mail this completed Incident Report to the following address:

California Information Security Office
P.O. Box 1810, Mail Stop Y-12
Rancho Cordova, CA 95741-1810

[ORGANIZATION NAME]

Org Address
Org Address

Mr & Mrs Citizen
1234 Any Street
Any City, ST 99999

Notice of Data Breach

Dear Mr & Mrs Citizen,

What Happened:
We are writing to you because of a recent security incident at [name of organization]. [Describe what happened in general terms, when it happened, specifically what kind of personal information was involved, and what you are doing in response. If the breach does not involve Social Security number, driver's license/California Identification Card, or financial account numbers, say so. Refer to the following language.]

What Information Was Involved:
Please note, the information was limited to [specify, (e.g., your name and medical treatment)] and did not contain any other information, such as Social Security number, Driver's License number, or financial account numbers which could expose you to identity theft.

What We Are Doing:
Nonetheless, we felt it necessary to inform you since your medical information [or medical history, medical condition, or medical treatment or diagnosis] was involved.

What you can do:
Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your [provider or plan], to serve as a baseline.

Other Important Information:
For information about your medical privacy rights, you may visit the website of the California Department of Justice, Privacy Enforcement and Protection at www.privacy.ca.gov.
We regret that this incident occurred and want to assure you we are reviewing and revising our procedures and practices to minimize the risk of recurrence.

For More Information:
Should you need any further information about this incident, please contact [name of the designated agency official or agency unit handling inquiries] at [toll-free phone number].

Sincerely,

Joe Government

DEPARTMENT OF DEVELOPMENTAL SERVICES

COMMUNITY OPERATIONS DIVISION
PROGRAM ADVISORY

COD 09-01 **November 2009**

SECURING CONFIDENTIAL INFORMATION AND DATA

INTRODUCTION

This program advisory provides updated notification requirements for privacy breaches and security incidents. This advisory supersedes the Program Advisory dated August 2008 on Securing Confidential Information and data.

PURPOSE

This program advisory provides information on best practices for protecting confidential, sensitive, and personal information (information)[1], regardless of format (i.e., electronic or paper); This advisory also provides updated guidance on required notification to the Department of Developmental Services (DDS) when this information has been lost or inadvertently released to unauthorized persons OR when there has been a loss of state-owned assets (cell phones, PDAs, laptops, desktop computers, etc.)

SECURING INFORMATION IN BOTH PAPER AND ELECTRONIC FORMATS

The California Office of Information Security and Privacy Protection (OISPP) establishes best practice policies that State Information Technology (IT) entities such as DDS are mandated to implement. On September 6, 2006, Management Memo 06-12 mandated requirements for protecting all confidential, sensitive, and/or personal information regardless of format or media type. It also revised incident reporting requirements to include inappropriate or unauthorized access, use, or disclosure of information whether in paper or electronic format.

This policy applies to all confidential, sensitive, and/or personal information collected and stored on behalf of the State by *employees, vendors, **contractors,** or researchers*.

DDS recommends that regional centers, as DDS contractors, implement equivalent "best practice" policies and procedures to meet legal and policy mandates (e.g., Management Memo referenced above and HIPAA). Regional centers are also responsible for ensuring all vendors/business partners, to whom this applies, are made aware of this information.

RECOMMENDED BEST PRACTICE GUIDELINES FOR REGIONAL CENTER CONSIDERATION/USE

Implement appropriate safeguards to prevent unauthorized use or disclosure of information:

- Secure information in locked rooms or cabinets;
- Do not leave information in places, such as conference rooms, where unauthorized persons could access it;
- Do not leave laptops, mobile media devices, cell phones or paper documents in automobiles;
- Shred documents with sensitive information instead of throwing them away in the garbage;
- Double check fax numbers prior to sending information out; coordinate a system to confirm receipt by the person to whom the information was sent;
- Encrypt information sent via email or provide as a password protected attachment and send the password in a separate communication;
- When possible, use registered mail to send information to confirm it wasn't intercepted or delivered to the wrong party;
- Do not store confidential, sensitive, or personal data on *non-encrypted* laptops or mobile devices.
- Do not backup data to *non-encrypted* media such as diskettes, memory sticks, or CDs.
- Ensure agreements with vendors or other contractors include assurances to appropriately protect information to prevent future privacy breaches or security incidents.

NOTIFICATION REQUIREMENTS

The law requires the reporting of privacy breaches and security incidents involving paper and other formats. Immediately notify DDS' Information Security Officer, Carol Risley via email at crisley@dds.ca.gov in the event of any loss or theft of personal, sensitive, or confidential information in any format, including but not limited to flash drives, cell phones, personal digital assistants (i.e. blackberry), computers, and laptops.

The notification to DDS must be reported on the attached form (SIMM 65C) and contain all the information outlined below. *DDS is mandated by law to notify other entities of disclosure of information; the timelines are extremely short for many of these reports; **therefore it is essential***

that centers notify DDS as soon as they learn of an incident and complete and submit the SIMM 65C.

DDS will need all of the following information upon notification of such an incident:

1. Date incident occurred. If unknown, so indicate.
2. Date incident was detected. If unknown, so indicate.
3. Location (physical address) of incident.
4. Description of incident (what and how it happened).
5. Media/device type (if applicable).
6. Serial and state asset number of any equipment.
7. Was portable storage device encrypted (if applicable), if not explain.
8. If local law enforcement was notified, include the name of the agency; report number; and, the name, telephone number and badge number of the officer taking the report.
9. Costs associated with resolving this incident, (i.e. equipment, mailing of privacy notices, etc.)
10. If incident involved personally identifiable information:
    a. What type of personally identifiable information was involved (if applicable) (name, social security number, driver's license/State ID number, health or medical information, financial information, other). Include all that apply.
    b. Is a privacy disclosure notice required? If so, attach a sample of the notification letter. Redact personal information such as name, address, etc.
    c. Individual(s) eligible for TCM and/or HCBS Waiver services?
    d. Number of individuals affected?
    e. Date notification(s) were made (if applicable).
11. Corrective actions taken to prevent future occurrences.
12. Estimated costs of those corrective actions.
13. Date corrective actions will be fully implemented.

OISPP requires State departments to submit notification letters to them for approval prior to notifying impacted individuals on loss of confidential information. DDS has received approval by OISPP to utilize the attached templates instead of going through the OISPP approval process every time there is a loss, which will save considerable time and resources. Each template allows for reporting the unauthorized disclosure of different types of information. To avoid confusion, the template designed for reporting the disclosure of particular information must be used. For example, there is a template for reporting the unauthorized disclosure of social security numbers. In addition to using these standard templates when reporting breaches to DDS, regional centers may also want to share these templates with vendors for their use in reporting breaches to regional centers. Standardized use of these templates across the system will assist in ensuring complete, proper and timely notification of consumers when a breach occurs and efficient and complete reporting to regional centers, DDS and other required entities.

If your regional center chooses to utilize a different format or verbiage, it must be approved by OISPP prior to dissemination. Failure to have OISPP approval could increase workload for all regional centers and DDS; as well as invite increased oversight of OISPP, including on-site visits.

If you have any questions regarding securing confidential information or state-owned assets; or reporting security incidents, please contact: DDS Security Officer, Carol Risley, at (916) 654-1888 or DDS Privacy Officer, Cindy Bosco, at (916) 654-0123.

---

[1] For the terms "*confidential, sensitive, personal,*" DDS uses the definitions circulated by the Department of Finance and found in the State Administrative Manual.

Confidential Information: information maintained by state agencies that is exempt from disclosure under the provisions of the California Public Records Act (Government Code Sections 6250-6265) or other applicable state or federal laws.

Sensitive Information: information maintained by state agencies that requires special precautions to protect from unauthorized use, access, disclosure, modification, loss, or deletion. Sensitive information may be either public or confidential. It is information that requires a higher than normal assurance of accuracy and completeness. Thus the key factor for sensitive information is that of integrity. Typically, sensitive information includes records of agency financial transactions and regulatory actions.

Personal Information: information that identifies or describes an individual as defined in, but not limited by, the statutes listed below. This information must be protected from inappropriate access, use, or disclosure and must be made accessible to data subjects upon request: a. Notice-triggering personal information – specific items or personal information (name plus Social Security Number, driver's license/California identification card number, or financial account number) that may trigger a requirement to notify individuals if an unauthorized person acquires it. See Civil Code Sections 1798.29 and 1798.3, b. Protected Health Information – individually identifiable information created, received, or maintained by such organizations as health care payers, health care providers, health plans, and contractors to these entities, in electronic or physical form. State law requires special precautions to protect from unauthorized use, access or disclosure. See Confidentiality of Medical Information Act, Civil Code Section 56 et seq. and the Patients' Access to Health Records Act, Health and Safety Code Sections 123100-123149.5; and, c. Electronic Health Information – individually identifiable health information transmitted by electronic media or maintained in electronic media. Federal regulations require state entities that are health plans, health care clearinghouses, or health care providers that conduct electronic transactions to ensure the privacy and security of electronic protected health information from unauthorized use, access, or disclosure. See Health Insurance Portability and Accountability Act, 45 C.F.R. parts 1

Privacy Protection Recommendations

What to Do If Your Personal Information Is Compromised

1 Contact the three credit bureaus.

You can report the potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus. You will also be sent instructions on how to get a copy of your report from each of the credit bureaus. As a possible victim of identity theft, you will not be charged for these copies.

Trans Union 1-800-680-7289 Experian 1-888-397-3742 Equifax 1-800-525-6285

2 What it means to put a fraud alert on your credit file.

A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that there may be fraud on the account. This alerts the merchant to take steps to verify the identity of the applicant. A fraud alert lasts 90 days and can be renewed.

3 Review your credit reports. Look through each one carefully.

Look for accounts you don't recognize, especially accounts opened recently. Look in the inquiries section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store names. The credit bureau will be able to tell you when that is the case. You may find some inquiries identified as "promotional." These occur when a company has obtained your name and address from a credit bureau to send you an offer of credit. Promotional inquiries are not signs of fraud. (You are automatically removed from lists to receive unsolicited offers of this kind when you place a fraud alert.) Also, as a general precaution, look in the personal information section for any address listed for you where you've never lived.

4 If you find items you don't understand on your report, call the credit bureau at the number on the report.

Credit bureau staff will review your report with you. If the information can't be explained, then you will need to call the creditors involved and report the crime to your local police or sheriff's office. For more information on what to do in this case, visit the California Office of Privacy Protection's Web site at www.privacy.ca.gov, and go to the Identity Theft page.

Cómo proteger su privacidad

Qué hacer si su información personal está comprometida

1 Póngase en contacto con las tres agencias de crédito.

Para informar el robo potencial de su identidad llame sin cargo a cualquiera de las tres agencias principales de crédito indicados a continuación. Accederá a un sistema telefónico automatizado para informar fraude el cual le permitirá marcar su archivo de crédito en las tres agencias de crédito con un alerta de fraude. También le enviarán instrucciones para solicitar una copia de su informe de cada una de las agencias de crédito. No tendrá que pagar por las copias del informe ya que se trata de un posible robo de identidad.

Trans Union 1-800-680-7289 Experian 1-888-397-3742 Equifax 1-800-525-6285

2 Qué quiere decir poner un alerta de fraude en su archivo de crédito.

Un alerta de ayudará a protegerlo contra la posibilidad de que un ladrón de identidad abra cuentas nuevas de crédito en su nombre. Cuando un comerciante verifica el historial de crédito de una persona que está solicitando crédito, recibirá un aviso indicando que puede haber fraude en la cuenta. Esto alerta al comerciante a que tome pasos para verificar la identidad del solicitante. El alerta de fraude dura 90 días y se puede renovar.

3 Examine sus informes de crédito. Revise cuidadosamente cada uno de ellos.

Fíjese si hay cuentas que no reconoce, sobre todo cuentas abiertas recientemente. Fíjese en la sección de consultas para ver si hay empresas a las que no les solicitó crédito. Algunas empresas facturan bajo un nombre distinto que el nombre de la empresa. En esos casos, la agencia de crédito podrá aclarar de qué empresa se trata. Puede encontrar ciertas consultas identificadas como "promocionales". Estas consultas son efectuadas cuando una compañía obtuvo su nombre y dirección de una agencia de crédito y le envía una oferta de crédito. Las consultas promocionales no son un signo de fraude. (Cuando haga un alerta de fraude, lo eliminarán automáticamente de las listas de ofertas no solicitadas de este tipo). Como precaución general, fíjese también en la sección sobre información personal para ver si hay alguna dirección donde nunca ha vivido.

4 Si encuentra en su informe transacciones que no comprende, llame a la agencia de crédito al número que aparece en el informe.

El personal de la agencia de crédito analizará el informe junto con usted. Si no puede explicar la información usted tendrá que llamar a los acreedores involucrados e informar el delito en su comisaría u oficina del alguacil local. Para obtener más información sobre lo que tiene que hacer en este caso, visite el sitio Web de la Oficina de Protección de Privacidad de California en www.privacy.ca.gov y vaya a la página de Robo de identidad *(Identity Theft)*.