

---

## 23. COMPLIANCE

### A. Fraud, Waste and Abuse Program

---

#### **APPLIES TO:**

- A. This policy applies to all IEHP Medicare DualChoice (HMO SNP) Providers.

#### **POLICY:**

- A. IEHP believes that Compliance with fraud prevention and reporting is everyone's responsibility.
- B. IEHP has developed a Fraud, Waste and Abuse Program (FWA) to comply with the Centers for Medicare and Medicaid Services (CMS) Medicare Advantage requirements in preventing and detecting fraud in federal and state funded programs.
- C. The objective of IEHP's FWA is to identify and reduce costs caused by fraudulent activities and to protect consumers, Members, health care providers and others in the delivery of health care services.
- D. Providers are educated regarding the federal and state false claims statutes and the role of such laws in preventing and detecting fraud, waste and abuse in federal health care programs.
- E. IEHP has created a Compliance Committee (CC) to oversee its FWA and to manage all instances of suspected fraud.
- F. All activities of the CC are confidential to the extent permitted by law.
- G. IEHP reports its fraud prevention activities and suspected fraud to regulatory and law enforcement agencies as required by law.
- H. Providers must adhere to federal and California State laws, including but not limited to False Claims laws.
- I. Providers with IEHP will comply with federal and California State laws in regards to the detection, reporting, and investigation of suspected fraud and abuse.

#### **DEFINITIONS:**

- A. A complaint of fraud, waste and/or abuse is a statement, oral or written, alleging that a practitioner, supplier, or beneficiary received a benefit to which they are not otherwise entitled. Included are allegations of misrepresentations and violations of Medicare, Medicaid or other health care program requirements applicable to persons applying for covered services, as well as the lack thereof of such covered services.
- B. Fraud and abuse differ in that:
1. Abuse applies to practices that are inconsistent with sound fiscal, business, medical or recipient practices and result in an unnecessary cost to a health care

---

## 23. COMPLIANCE

### A. Fraud, Waste and Abuse Program

---

program, or in reimbursement for services that are not medically necessary or that fail to meet professionally recognized standards for health care. Mistakes that are repeated after discovery or represent an on-going pattern could constitute abuse.

2. Fraud is an intentional or knowing misrepresentation made by a person with the knowledge (or knowingly) that the deception could result in some unauthorized benefit to him/herself or another person. It includes any portion that constitutes fraud under applicable federal or state law. Mistakes that are not committed knowingly or that are a result of negligence are not fraud, but could constitute abuse

#### **REFERENCES:**

- A. Code of Federal Regulations, Title 42, Part 423
- B. Code of Federal Regulations, Title 42, §455.2
- C. Federal False Claims Act, US Code, Title 31

#### **PROCEDURE:**

- A. IEHP's FWA Program is designed to deter, identify, investigate and resolve potential fraudulent activities that may occur in IEHP daily operations, both internally and externally.
- B. The Chief Compliance Officer is responsible for ensuring that the objectives of IEHP's Fraud, Waste and Abuse Program are carried out, and for preventing, detecting and investigating fraud-related issues in a timely manner. To accomplish this, the Chief Compliance Officer designates and oversees the Compliance Department to perform the following responsibilities:
  1. Developing fraud training programs to educate staff, Providers, practitioners, Members and down-stream entities on prevention, deterrence and detection of fraud, waste and abuse.
  2. Identifying, detecting, thoroughly investigating, managing and resolving all suspected instances of fraud, waste, and abuse, waste and abuse internally and externally.
  3. Cooperating with, reporting and referring suspected fraud, waste and abuse to the appropriate governmental and law enforcement agencies, as applicable, including exchange of information as appropriate.
- C. Both IEHP and Providers have responsibilities for fraud prevention.
- D. IEHP responsibilities include, but are not limited to the following:

---

## 23. COMPLIANCE

### A. Fraud, Waste and Abuse Program

---

1. Training IEHP staff, Providers, practitioners, Members and vendors on fraud, IEHP Fraud, Waste and Abuse Program, and fraud prevention activities at least annually.
2. Communicating its FWA and efforts through IEHP University, the IEHP Provider Policy and Procedure Manual, IEHP Provider Newsletter, Joint Operation Meetings, targeted mailings or in-service meetings.
3. Continuous monitoring and oversight, both internally and externally, of daily operational activities to detect and/or deter fraudulent behavior. Such activities include, but are not limited to:
  - a. Monitoring of Member grievances
  - b. Monitoring of Provider and physician grievances
  - c. Claims Audits and monitoring activities, including audits of the P4P Program and other direct reimbursement programs to physicians
  - d. Review of Providers' financial statements
  - e. Medical Management Audits
  - f. Utilization Management monitoring activities
  - g. Quality Management monitoring activities
  - h. Case Management Oversight activities
  - i. Pharmacy Audits
  - j. Encounter Data Reporting Edits
  - k. Chart Audits
  - l. Clinical Audits
4. Investigating and resolving all reported and/or detected suspected instances of fraud and taking action against confirmed suspected fraud, waste, and abuse including but not limited to reporting to law enforcement agencies, termination of the IEHP contract (if a Provider, direct contracting practitioner, or vendor), and/or removal of a participating practitioner from the IEHP network. IEHP reports suspected fraud to the following entities, as deemed appropriate and required by law:
  - a. The Centers for Medicare and Medicaid Services (CMS)
  - b. The Federal Office of the Inspector General (Medicaid/Medicare Fraud)
  - c. Medical Board of California (MBOC)
  - d. Local law enforcement agencies

---

## 23. COMPLIANCE

### A. Fraud, Waste and Abuse Program

---

5. Submitting periodic reports to CMS as required by law.
  6. Encouraging and supporting Provider activities related to fraud prevention and detection.
- E. The Providers' responsibilities for fraud prevention and detection include, but are not limited to, the following:
1. Training Provider staff, contracting physicians and other affiliated or ancillary providers, and vendors on IEHP and Provider's Fraud, Waste and Abuse Program and fraud, waste and abuse prevention activities and false claims laws at least annually.
  2. Verifying and documenting the presence/absence of contracted individuals and/or entities by accessing the following online site prior to contracting and periodically thereafter: [www.oig.hhs.gov/fraud/exclusions.asp](http://www.oig.hhs.gov/fraud/exclusions.asp).
  3. Terminating the IEHP Medi-Cal network participation of individuals and entities who appear on the Office of Inspector General (OIG) List of Excluded Individuals and Entities (LEIE).
  4. Developing a FWA Program, implementing fraud, waste and abuse prevention activities and communicating such program and activities to contractors and subcontractors.
  5. Communicating awareness, including:
    - a) Identification of fraud, waste and abuse schemes.
    - b) Detection methods and monitoring activities to contracted and subcontracted entities and IEHP.
  6. Notifying IEHP of suspected fraudulent behavior and asking for assistance in completing investigations.
  7. Taking action against suspected or confirmed fraud, waste and abuse including referring such instances to law enforcement and reporting activity to IEHP.
  8. Policing and/or monitoring own activities and operations to detect and/or deter or prevent fraudulent behavior.
  9. Cooperating with IEHP in fraud, waste and abuse detection and awareness activities, including monitoring, reporting, etc., as well as cooperating with IEHP in fraud, waste and abuse investigations to the extent permitted by law
  10. Prompt return of identified overpayments of state and/or federal claims.
- F. Reporting Concerns Regarding Fraud, Waste Abuse and False Alarms
1. IEHP takes issues regarding false claims and fraud, waste and abuse seriously. IEHP providers, and their contractors or agents of IEHP's providers are to be

---

## 23. COMPLIANCE

### A. Fraud, Waste and Abuse Program

---

aware of the laws regarding fraud, waste and abuse and false claims and to identify and resolve any issues immediately. Affiliated providers' employees, managers, and contractors are to report concerns to their immediate supervisor when appropriate.

2. IEHP provides the following ways in which to report alleged and/or suspected fraud, waste and/or abuse directly to the plan:

a. In writing to:

Chief Compliance Officer

IEHP

P.O. Box 19026

San Bernardino, CA 92423-9026

b. By E-mail to: [compliance@iehp.org](mailto:compliance@iehp.org)

c. By toll free number: (866) 355-9098 (Compliance Hot Line)

d. By fax to: (909) 890-2973

3. The Suspected Noncompliance/Fraud Report Form is to be completed when reporting concerns regarding fraud, waste, abuse and false claims (See Attachment 23-1 in Section 23 "Attachments"). The form is also available on the IEHP website.

4. The following information is needed in order for IEHP to investigate suspected fraud, waste and/or abuse:

a. Your name. Although you may choose to report anonymously, it is very helpful for the IEHP Compliance Department to hear the allegations directly from you. If you choose to give your name, please provide a contact number and a date and time for a return call at a time and place confidential for you.

b. The name(s) of the party/parties/departments involved in the suspected fraud.

c. Where the suspected fraud may have occurred.

d. Details on the suspected criminal activity.

e. When the suspected fraud took place, for example over what period of time.

f. A description of any documentation in your possession that may support the allegation of fraud, waste and/or abuse.

---

## 23. COMPLIANCE

### A. Fraud, Waste and Abuse Program

---

5. Information reported to the IEHP Fraud Prevention Program will remain confidential to the extent possible by law.

INLAND EMPIRE HEALTH PLAN		
<b>Chief Approval:</b> <i>Signature on file</i>	<b>Effective date:</b>	January 1, 2007
<b>Chief Title:</b> Chief Executive Officer	<b>Revised date:</b>	January 1, 2011

---

## 23. COMPLIANCE

### B. HIPAA Protected Health Information

---

#### **APPLIES TO:**

- A. This policy applies for all IEHP Medicare DualChoice (HMO SNP) Members and Providers.

#### **POLICY:**

This policy is based on the following principles and procedures related to the access, use and disclosure of Member information.

- A. To provide guidance regarding each provider's responsibility related to identifiable Member information. This policy addresses an intentional or unintentional breach of Member confidentiality, including oral, written and electronic communication. This definition will safeguard Member privacy and help minimize exposure and/or liability to Members, providers, facilities and IEHP.
- B. Providers must make reasonable efforts to safeguard the privacy and security of Members' PHI and are responsible for adhering to this policy by using only the minimum information necessary to perform his or her responsibilities, regardless of the extent of access provided or available.
- C. Providers must comply with the federal Health Insurance Portability and Accountability Act ("HIPAA") laws and regulations including, but not limited to the privacy and security of Members' protected health information ("PHI") as required by the Health Insurance Portability and Accountability Act ("HIPAA"), Standards for Privacy of Members' Identifiable Health Information, 45 CFR Parts 160 and 164; the administrative, physical, and technical safeguards of the HIPAA Security Rule, as required by the Health Information Technology for Economic and Clinical Health Act (HITECH Act) as part of the American Recovery and Reinvestment Act of 2009; and any and all Federal regulations and interpretive guidelines promulgated there under.
- D. Providers are allowed to release Member PHI to IEHP, without prior authorization from the Member, if the information is for treatment, payment or health care operations related to IEHP plans or programs.
- E. Providers must notify IEHP, their Members; the Centers for Medicare and Medicaid (CMS); and, the U.S. Department of Health & Human Services (DHHS) of any suspected or actual breach regarding the privacy and security of a Member's PHI within prescribed timelines and through electronic submission formats.
- F. **Definition:**  
"Protected Health Information" or "PHI" means any information, whether oral or recorded in any form or medium that relates to the past, present, or future physical or mental 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

---

## 23. COMPLIANCE

### B. HIPAA Protected Health Information

---

identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual. PHI shall have the meaning given to such term under HIPAA and HIPAA regulations, as the same may be amended periodically.

#### **PROCEDURE:**

- A. Only providers and their respective staff members with a legitimate “need to know” may access, use or disclose member information. This includes all activities related to treatment, payment and health care operations on behalf of IEHP. Each provider and their respective staff members may only access, use or disclose the minimum information necessary to perform his or her designated role regardless of the extent of access provided to him or her.
- B. With respect to system access, member privacy will be supported through authorization, access, and audit controls (e.g., roles-based access) and should be implemented for all systems that contain identifying member information. Within the permitted access, a member system user is only to access what they need to perform his or her job.
- C. Each provider is responsible for attending ongoing education on member privacy and member rights as directed.
- D. Each provider is responsible for compliance with these Protected Health Information policies and principles.
- E. Permitted Uses and Disclosures
  - 1. Except as otherwise required by law, Providers are allowed to release Member information, including PHI, without Member authorization, to IEHP for treatment, payment, or health care operations related to IEHP plans or programs.
  - 2. Activities which are for purposes directly connected with the administration of services include, but are not limited to:
    - a. Establishing eligibility and methods of reimbursement;
    - b. Determining the amount of medical assistance;
    - c. Arranging or providing services for Members;
    - d. Conducting or assisting an investigation, prosecution, or civil or criminal proceeding related to the administration of IEHP plans or programs;
    - e. Conducting or assisting in an audit related to the administration of IEHP plans or programs.
- F. Reporting of Improper Disclosures
  - 1. Providers are required to report unauthorized disclosures to:

---

## 23. COMPLIANCE

### B. HIPAA Protected Health Information

---

- a. The U.S. Department of Health & Human Services (DHHS), for breaches of unsecured PHI, sent electronically without unreasonable delay and in no case later than sixty (60) days from discovery of a breach affecting 500 or more individuals; and, electronic notice sent annually by March 1st for DHHS defined breaches that have occurred during the previous year that affected fewer than 500 individuals (see Attachment 23-2). Please see Attachment 23-3 for electronic submission of breaches affecting 500 or more individuals to DHHS. For annual reportable breaches affecting fewer than 500 individuals, see Attachment 23-4, or access the DHHS Website: <http://transparency.cit.nih.gov/breach/index.cfm>.
- b. The IEHP Member(s) whose PHI has been breached in accordance with CMS and DHHS requirements.
- c. The IEHP Chief Compliance Officer within the regulatory timeline requirements of CMS and DHHS. Copies of the electronic submissions sent to CMS and/or DHHS may be sent to IEHP as notification of Member breaches.

**IEHP Chief Compliance Officer**

Inland Empire Health Plan

P.O. Box 19026

San Bernardino, CA 92423-9026

Toll Free Compliance Hotline: (866) 355-9098

Fax: (909) 890-2973

E-mail: [compliance@iehp.org](mailto:compliance@iehp.org)

2. Providers must take prompt corrective action to mitigate and cure the cause(s) of the the unauthorized disclosure.

INLAND EMPIRE HEALTH PLAN		
<b>Chief Approval:</b> <i>Signature on file</i>	<b>Effective date:</b>	January 1, 2007
<b>Chief Title:</b> Chief Executive Officer	<b>Revised date:</b>	January 1, 2012

---

## 23. QUALITY MANAGEMENT

### C. Health Care Professional Advice to Members

---

**APPLIES TO:**

- A. This policy applies to all IEHP Medicare DualChoice (HMO SNP) Members.

**POLICY:**

- A. IEHP and contracted partners shall not prohibit or restrict a health care professional acting within their professional scope of work, from advising or advocating on behalf of a Member whom they are caring for.

**PROCEDURE:**

- A. A health care professional shall be able to give advice or advocate for a Member regarding the Member's:
1. Health Status;
  2. Medical Care;
  3. Treatment options, which include:
    - a. Self-administered alternative treatments; and
    - b. Adequate information to make a decision against treatment options;
  4. Risks and benefits of such treatments or non-treatments;
  5. Right to refuse treatment; and
  6. Right to express preferences about future treatment decisions.
- B. A health care professional shall provide to a Member treatment options, including the option of no treatment, in a culturally competent manner. A health care professional shall ensure a Member with a disability has effective communications, with participants throughout the health system, in making decisions regarding treatment options.
- C. IEHP shall inform Members of their right to refuse treatment and information regarding advance directives in accordance with Policy 7D, "Durable Power of Attorney for Healthcare."
- D. If a contracted provider violates the terms of this policy, they will be subject to contract termination.

<b>INLAND EMPIRE HEALTH PLAN</b>		
<b>Chief Approval:</b> <i>Signature on file</i>	<b>Effective date:</b>	January 1, 2007
<b>Chief Title:</b> Chief Medical Officer	<b>Revised date:</b>	

---

## 23. COMPLIANCE

### Attachments

---

<u>ATTACHMENT</u>	<u>DESCRIPTION</u>	<u>POLICY CROSS REFERENCE</u>
23-1	Suspected Fraud Report Form	23A
23-2	HITECH Breach Notification Grid	23B
23-3	DHHS PB Notification For Affecting 500 or more individuals	23B
23-4	DHHS PB Notification Form Affecting Less than 500 individuals	23B



INLAND EMPIRE HEALTH PLAN

### SUSPECTED NONCOMPLIANCE / FRAUD REPORT FORM

Date Submitted \_\_\_\_\_ Date of Incident \_\_\_\_\_  
 Reported by (Your Name) \* \_\_\_\_\_  
 Your Organization \* \_\_\_\_\_

\* This form can be completed and submitted anonymously, if necessary.

**Type of Allegation: (Check all that apply)**

<input type="checkbox"/> ID Card	<input type="checkbox"/> Utilization	<input type="checkbox"/> Medical Records
<input type="checkbox"/> Prescription/Pharmacy	<input type="checkbox"/> Claims/Billing/Capitation	<input type="checkbox"/> Credit Card
<input type="checkbox"/> Eligibility	<input type="checkbox"/> Encounter/Data/Data Reporting	<input type="checkbox"/> Financial
<input type="checkbox"/> Enrollment/Disenrollment	<input type="checkbox"/> TPL/Co-Insurance/COB	<input type="checkbox"/> Purchasing/Bidding
<input type="checkbox"/> Referrals/Denial	<input type="checkbox"/> Credentialing/Licensing	<input type="checkbox"/> Marketing
	<input type="checkbox"/> Other _____	

**Fraud Involves: (Check all that apply)**

<input type="checkbox"/> Member	<input type="checkbox"/> Practitioner	<input type="checkbox"/> Provider
<input type="checkbox"/> IEHP Team Member	<input type="checkbox"/> IEHP Vendor	<input type="checkbox"/> Other _____

Name: \_\_\_\_\_ ID#: \_\_\_\_\_  
 Do you have documentation in your possession, which could be used as evidence? Yes  No   
 Is the documentation attached to this report? No  Yes   
 Have you previously reported this? No  Yes  to whom: \_\_\_\_\_

**Describe the potential fraudulent activity** (attach extra sheet, if necessary):

Law Enforcement has been contacted? Yes  No   
 Date Reported: \_\_\_\_\_ Report Number: \_\_\_\_\_  
 Contact Information: \_\_\_\_\_

State Regulatory Agency contacted? Yes  No   
 Date Reported: \_\_\_\_\_ Report Number: \_\_\_\_\_  
 Contact Information: \_\_\_\_\_  
 Resolution: \_\_\_\_\_

Report N



### **Breaches Affecting Fewer than 500 Individuals**

For breaches that affect fewer than 500 individuals, a covered entity must provide the Secretary with notice annually. All notifications of breaches occurring in a calendar year must be submitted within 60 days of the end of the calendar year in which the breaches occurred. Notifications of all breaches occurring after the effective date in 2009 must be submitted by March 1, 2010. This notice must be submitted electronically by following the link below and completing all information required on the breach notification form. A separate form must be completed for every breach that has occurred during the calendar year.

If a covered entity that has submitted a breach notification form to the Secretary discovers additional information to report, the covered entity may submit an additional form, checking the appropriate box to signal that it is an updated submission.

# U.S. Department of Health & Human Services

*Improving the health, safety, and well-being of America*

## Health Information Privacy

Form Approved OMB No. 0990-0346

### Notice to the Secretary of HHS of Breach of Unsecured Protected Health Information

**Breach Affecting:**

**Report Type:**

500 or More Individuals

Initial Breach Report

Less Than 500 Individuals

Addendum to Previous Report

#### Section 1 - Covered Entity

Name of Covered Entity:

Address:

City:

State:

Zip Code:

Contact Name:

Contact Phone:

Contact E-mail:

Type of Covered Entity:

#### Section 2 –Business Associate. Complete this section if breach occurred at or by a Business Associate.

Name of Business Associate:

Address:

City:

State:

Zip Code:

Business Associate Contact Name:

Business Associate Contact Phone:

Business Associate Contact E-mail:

#### Section 3 –Breach

Date(s) of Breach: MM/DD/YYYY

Date(s) of Discovery: MM/DD/YYYY

Approximate Number of Individuals Affected by the Breach: 0

Type of Breach: Please select the type of breach. If type breach is "Other", please describe the type of breach in field below.

- Theft
- Loss
- Improper Disposal
- Unauthorized Access/Disclosure
- Hacking/IT Incident
- Unknown

Type of Breach (Other):

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

- Laptop
- Desktop Computer
- Network Server
- E-mail
- Other Portable Electronic Device

("Press Ctrl for Multiple Selections")

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 in the Description section below.

- Demographic Information
- Financial Information
- Clinical Information
- Other

("Press Ctrl for Multiple Selections")

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

- Firewalls
- Packet Filtering (router-based)
- Secure Brower Sessions
- Strong Authentication
- Encrypted Wireless

breach. ("Press Ctrl for Multiple Selections")

### Section 4 – Notice of Breach and Actions Taken

Date(s) Individual Notice Provided: MM/DD/YYYY

Was Substitute Notice Required?  Yes  No

Was Media Notice Required?  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 actions taken in the section below.

Security and/or Privacy Safeguards  
Mitigation  
Sanctions  
Policies and Procedures  
Other

("Press Ctrl for Multiple Selections")

**Describe Other Actions Taken:** Please describe in detail any actions taken following the breach in addition to those selected above.

## Section 5 – Attestation

Under the Freedom of Information Act (5 U.S.C. §552) and HHS regulations at 45 C.F.R. Part 5, OCR may be required to release information provided in your breach notification. For breaches affecting more than 500 individuals, some of the information provided on this form will be made publicly available by posting on the HHS web site pursuant to § 13402(e)(4) of the Health Information Technology for Economic and Clinical Health (HITECH) Act (Pub. L. 111-5). Additionally, OCR will use this information, pursuant to § 13402(j) of the HITECH Act, to provide an annual report to Congress regarding the number and nature of breaches that are reported each year and the actions taken to respond to such breaches. OCR will make every effort, as permitted by law, to protect information that identifies individuals or that, if released, could constitute a clearly unwarranted invasion of personal privacy.

**I attest, to the best of my knowledge, that the above information is accurate.**

**Name:** \_\_\_\_\_ **Date:** MM/DD/YYYY \_\_\_\_\_

(Typing your name represents your signature.)

Submit

**Burden Statement** Public reporting burden for the collection of information on this complaint form is estimated to average 15 to 30 minutes per response, including the time for reviewing instructions, gathering the data needed and entering and reviewing the information on the completed complaint form. An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a valid control number. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to: HHS/OS Reports Clearance Officer, Office of Information Resources Management, 200 Independence Ave. S.W., Room 531H, Washington, D.C. 20201.

(2/10)

[HHS Home](#) | [Frequent Questions](#) | [Contacting HHS](#) | [Accessibility](#) | [Privacy Policy](#) | [FOIA](#) | [Disclaimer](#) | [USA.gov](#) | [Helping America's Youth](#)

U.S. Department of Health & Human Services · 200 Independence Avenue, S.W. · Washington, D.C. 20201

### **Breaches Affecting 500 or More Individuals**

If a breach affects 500 or more individuals, a covered entity must provide the Secretary with notice of the breach without unreasonable delay and in no case later than 60 days from discovery of the breach. This notice must be submitted electronically by following the link below and completing all information required on the breach notification form.

If a covered entity that has submitted a breach notification form to the Secretary discovers additional information to report, the covered entity may submit an additional form, checking the appropriate box to signal that it is an updated submission.

**U.S. Department of Health & Human Services**  
*Improving the health, safety, and well-being of America*

**Health Information Privacy**

Form Approved OMB No. 0990-0346

**Notice to the Secretary of HHS of Breach of Unsecured Protected Health Information**

**Breach Affecting:**

**Report Type:**

500 or More Individuals

Initial Breach Report

Less Than 500 Individuals

Addendum to Previous Report

**Section 1 - Covered Entity**

Name of Covered Entity:

Address:

City:

State:

Zip Code:

Contact Name:

Contact Phone:

Contact E-mail:

Type of Covered Entity:

**Section 2 –Business Associate.** Complete this section if breach occurred at or by a Business Associate.

Name of Business Associate:

Address:

City:

State:

Zip Code:

Business Associate Contact Name:

Business Associate Contact Phone:

Business Associate Contact E-mail:

**Section 3 –Breach**

Date(s) of Breach: MM/DD/YYYY

Date(s) of Discovery: MM/DD/YYYY

Approximate Number of Individuals Affected by the Breach: 0

Type of Breach: Please select the type of breach. If type breach is "Other", please describe the type of breach in field below.

- Theft
- Loss
- Improper Disposal
- Unauthorized Access/Disclosure
- Hacking/IT Incident
- Unknown

Type of Breach (Other):

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

- Laptop
- Desktop Computer
- Network Server
- E-mail
- Other Portable Electronic Device

("Press Ctrl for Multiple Selections")

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 in the Description section below.

- Demographic Information
- Financial Information
- Clinical Information
- Other

("Press Ctrl for Multiple Selections")

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

- Firewalls
- Packet Filtering (router-based)
- Secure Brower Sessions
- Strong Authentication
- Encrypted Wireless

breach. ("Press Ctrl for Multiple Selections")

### Section 4 – Notice of Breach and Actions Taken

Date(s) Individual Notice Provided: MM/DD/YYYY

Was Substitute Notice Required?  Yes  No

Was Media Notice Required?  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 actions taken in the section below.

- Security and/or Privacy Safeguards
- Mitigation
- Sanctions
- Policies and Procedures
- Other

("Press Ctrl for Multiple Selections")

**Describe Other Actions Taken:** Please describe in detail any actions taken following the breach in addition to those selected above.



### Section 5 – Attestation

Under the Freedom of Information Act (5 U.S.C. §552) and HHS regulations at 45 C.F.R. Part 5, OCR may be required to release information provided in your breach notification. For breaches affecting more than 500 individuals, some of the information provided on this form will be made publicly available by posting on the HHS web site pursuant to § 13402(e)(4) of the Health Information Technology for Economic and Clinical Health (HITECH) Act (Pub. L. 111-5). Additionally, OCR will use this information, pursuant to § 13402(j) of the HITECH Act, to provide an annual report to Congress regarding the number and nature of breaches that are reported each year and the actions taken to respond to such breaches. OCR will make every effort, as permitted by law, to protect information that identifies individuals or that, if released, could constitute a clearly unwarranted invasion of personal privacy.

**I attest, to the best of my knowledge, that the above information is accurate.**

**Name:** \_\_\_\_\_ **Date:** MM/DD/YYYY \_\_\_\_\_

(Typing your name represents your signature.)

Submit

**Burden Statement** Public reporting burden for the collection of information on this complaint form is estimated to average 15 to 30 minutes per response, including the time for reviewing instructions, gathering the data needed and entering and reviewing the information on the completed complaint form. An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a valid control number. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to: HHS/OS Reports Clearance Officer, Office of Information Resources Management, 200 Independence Ave. S.W., Room 531H, Washington, D.C. 20201.

(2/10)