
23. COMPLIANCE

A. IPA Performance Evaluation

APPLIES TO:

- A. This policy applies to all IEHP Medi-Cal Providers.

POLICY:

- A. Annually IEHP evaluates each contracted IPA using the Performance Evaluation Tool (PET) to determine the overall performance and compliance with its IEHP contract, including compliance with IEHP policies and procedures.
- B. The PET is a standardized scoring mechanism that IEHP uses to evaluate and compare each IPA's health care delivery system and managed care capabilities in relation to compliance with IEHP standards.
- C. IEHP uses the PET to evaluate whether an IPA's contract should be renewed and to determine the length of term of an IPA's contract with IEHP, if applicable.

PROCEDURE:

- A. IEHP evaluates each IPA annually at least 180 days prior to the end of the contract year.
- B. IEHP reviews the following functional areas:
 - 1. Claims
 - 2. Communication
 - 3. Encounter Data
 - 4. Finance
 - 5. Grievances
 - 6. Delegation Oversight Audit Results
 - 7. IPA Reporting and Member Access Audit
- C. Each of the above categories is divided into specific subcategories. These subcategories describe the elements being scored, the frequency such data is collected, and the period of time being evaluated.
 - 1. For each element, IEHP has identified its expectations and the level (score) to be achieved (see Attachment 23-1 in Section 23, "Attachments" for a sample tool).
 - 2. The categories related to measures of an IPA's competence and quality of Member care (e.g., IPA Reporting and Member Access Audit and the IPA Delegation Oversight Audit Results) are weighted more heavily to ensure the IPAs maintain IEHP's quality standards and meet regulatory requirements.

23. COMPLIANCE

A. IPA Performance Evaluation

3. The data collected throughout the contract year is comprised of reports, summaries and scores of each IPA's performance and ability in meeting its delegated and non-delegated responsibilities, including results of monitoring and oversight activities, quality studies and medical management audits.
- D. IEHP uses the PET results to determine contract renewal terms (years) for each IPA. Term lengths are based on the following:
- | <u>Providers achieving total scores of:</u> | <u>Are awarded a contract term of:</u> |
|---|--|
| 95% or above | 3 years |
| 85% to 94.99% | 2 years |
| 80% to 84.99% | 1 year |
| Less than 80% | Non-renewal |
- E. IEHP meets with each IPA to discuss the results of its score and presents all relevant supporting documentation. This meeting can take place at the Joint Operations Meeting (JOM) or at a specific meeting called by IEHP.
- F. After a PET is completed for each contracted IPA, IEHP presents a summary to the IEHP Governing Board along with all relevant supporting documentation. This includes any IPA whose contract is not being renewed as a result of the PET score.
- G. IPAs whose contracts are being non-renewed are notified in writing by the IEHP CEO.
- H. IPAs that do not agree with the final outcome, may appeal to IEHP in accordance with Policy 16C, "Provider (IPA, Hospital and Practitioner) Grievance and Appeals Resolution Process."

INLAND EMPIRE HEALTH PLAN		
Chief Approval: <i>Signature on file</i>	Effective Date:	April 1, 1999
Chief Title: Chief Executive Officer	Revised Date:	January 1, 2012

23. COMPLIANCE

B. Fraud, Waste and Abuse Program

APPLIES TO:

- A. This policy applies to all IEHP 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 certain requirements set forth in the Deficit Reduction Act of 2005 with regard to federal and state false claims laws, the Department of Managed Health Care (DMHC) and in accordance with Health and Safety Code, Section 1348, enacted in 1998 through SB 956, as well as to meet the expectations of the federal and state government in preventing and detecting fraud in federal or state funded programs such as Medi-Cal.
- C. The objective of the IEHP 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 Medicaid or other health care program requirements applicable to persons applying for covered services, as well as the lack thereof of such covered services.

23. COMPLIANCE

B. Fraud, Waste and Abuse Program

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 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.

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
- D. California Code of Regulations, Title 22
- E. Health and Safety Code §1348
- F. DHCS Contract 04-35765

PROCEDURE:

- A. IEHP 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. IEHP's Chief Compliance Officer is responsible for ensuring that the objectives of IEHP FWA 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, waste and abuse training programs to educate staff, Providers, practitioners, Members and vendors on prevention, deterrence and detection of fraud, waste and abuse.

23. COMPLIANCE

B. Fraud, Waste and Abuse Program

2. Identifying, detecting, thoroughly investigating, managing and resolving all suspected instances of fraud, 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:
1. Training IEHP staff, Providers, practitioners, Members and vendors on fraud, IEHP FWA, and fraud, waste and abuse 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 PIP 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 or 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

23. COMPLIANCE

B. Fraud, Waste and Abuse Program

suspected fraud, waste or abuse to the following entities, as deemed appropriate and required by law:

- a. The California Department of Justice, Bureau of Medi-Cal Fraud
 - b. The California Department of Health Care Services (DHCS), Investigations Branch
 - c. The Centers for Medicare and Medi-Cal Services (CMS)
 - d. Department of Managed Health Care (DMHC)
 - e. Medical Board of California (MBOC)
 - f. Local law enforcement agencies
5. Submitting periodic reports to DHCS, DMHC, MRMIB or 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 (FWA) 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.
 3. Terminating the IEHP Medi-Cal network participation of individuals and/or 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.

23. COMPLIANCE

B. Fraud, Waste and Abuse Program

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 or 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 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
 - c. By toll free number: (866) 355-9038 (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 23-2 in Section 23, "Attachments" for a sample form). 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

23. COMPLIANCE

B. Fraud, Waste and Abuse Program

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

INLAND EMPIRE HEALTH PLAN		
Chief Approval: <i>Signature on file</i>	Effective date:	September 1, 1999
Chief Title: Chief Executive Officer	Revised date:	January 1, 2011

23. COMPLIANCE

C. HIPAA Federal and State Regulations for Protected Health Information (PHI)

APPLIES TO:

- A. This policy applies to all IEHP Medi-Cal 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 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 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 and the following regulatory agencies of any suspected or actual breach regarding the privacy and security of a Member's PHI within prescribed timelines and through electronic submission formats:
1. The California Department of Health Care Services (DHCS)
 2. The Secretary of the U.S. Department of Health & Human Services (DHHS)
- F. Definition:

23. COMPLIANCE

C. HIPAA Federal and State Regulations for Protected Health Information (PHI)

1. “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 member, the provision of health care to an member, or the past, present, or future payment for the provision of health care to an member; and that identifies the member or with respect to which there is a reasonable basis to believe the information can be used to identify the member. PHI shall have the meaning given to such term under HIPAA and HIPAA regulations, as the same may be amended periodically.
- G. Due to recent unauthorized disclosures of protected patient medical records, new confidentiality requirements were enacted by AB 211 and SB 541, effective 1/1/09. The bills make providers, accountable for unauthorized access to medical information, not just for unlawful use or disclosure.
1. Every provider of health care must implement appropriate administrative, technical, and physical safeguards to protect the privacy of a patient’s medical record information and safeguard it from unauthorized access or unlawful access, use, or disclosure. Administrative fines for violations range from \$25,000 to \$250,000.
 2. Due to the severity of the potential fines, all providers should educate their employees on privacy laws and their policy on privacy of medical information. The education should be documented and should include attendance. Appropriate, documented action must be taken should unauthorized access occur; and, an incident of unauthorized access must be reported to the California Department of Public Health and to the affected patient within five (5) days after detection of the breach.

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, an member system user is only to access what they need to perform his or her job.

23. COMPLIANCE

C. HIPAA Federal and State Regulations for Protected Health Information (PHI)

- 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; and
 - e. Conducting or assisting in an audit related to the administration of IEHP plans or programs.
- F. Providers are required to report unauthorized disclosures to:
 - 1. The California Department of Health Care Services (DHCS) within twenty-four (24) hours from the time that the breach was identified (Please see Attachment 23-3 in Section 23, “Attachments” for electronic submission to DHCS. This form can also be accessed on the IEHP Provider Website.)
 - 2. 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 23-4). Please see Attachment 23-5 for electronic submission of breaches affecting 500 or more individuals to DHHS. For annual reportable breaches affecting fewer than 500 individuals, see Attachment 23-6, or access the DHHS Website: <http://transparency.cit.nih.gov/breach/index.cfm>.
 - 3. The IEHP Member(s) whose PHI has been breached in accordance with DHCS and DHHS requirements.

23. COMPLIANCE

C. HIPAA Federal and State Regulations for Protected Health Information (PHI)

4. The IEHP Chief Compliance Officer within the designated timeline requirements of the applicable regulatory agency(ies). Copies of the electronic submissions sent to the applicable regulatory agency(ies) 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

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

INLAND EMPIRE HEALTH PLAN		
Chief Approval: <i>Signature on file</i>	Effective date:	August 1, 2006
Chief Title: Chief Executive Officer	Revised date:	January 1, 2012

23. COMPLIANCE

Attachments

<u>ATTACHMENT</u>	<u>DESCRIPTION</u>	<u>POLICY CROSS REFERENCE</u>
23-1	IPA Performance Evaluation Tool	23A
23-2	Suspected Fraud Report Form	23B
23-3	DHCS Privacy Breach Written Report	23C
23-4	DHHS PB Notification Form Affecting 500 or More Individuals	23C
23-5	DHHS PB Notification Form Affecting Less than 500 Individuals	23C
23-6	HITECH Breach Notification Grid	23C

**Inland Empire Health Plan
IPA Performance Evaluation Tool 2011/2012**

IPA NAME:		IPA CODE:			DATE:	
FUNCTIONAL AREA		Pts Poss	Raw Score	Pts Scored	IEHP Expectation	IEHP Scoring
I	CLAIMS				Total possible points:	20
1	Claims Audit – 03/11 - 02/12 (9 points)					
A	Audit Date: _____. What was the compliance level for the Annual Audit?	5			Must pass the audit as outlined in Audit Guide.	Pass=5, Conditional Pass =2, Non-Compliant=1, Fail=0
B	Were all Claims Universes submitted timely, accurately and completed in their entirety?	1			Provides Claims Universe by due date	YES=1; NO=0
C	Were all Claims Audit documents submitted timely, accurately and completed in their entirety?	1			Provides Audit Documents by due date	YES=1; NO=0
D	If the IPA received a Conditional Pass, Non-Complaint or Failed Score, how many CAPs were required?	1			No more than one CAP	0-1 CAP=1 >1 CAP=0
E	Were CAPs submitted timely?	1			Provides CAP by due date	YES=1; NO=0
F	Was a Verification Audit required at any time during the year?	1			No Verification Audit required during timeframe	0 Verification Audit =1; >1 Verification Audit=0
G	Was a Focused Audit required at any time during the year?	1			No Focused Audit required during timeframe	0 Focused Audit =1; >1 Focused Audit=0
2	Claims Reports – 03/11 - 02/12 (5 points)					
A	Were all monthly reports submitted timely, accurately and completed in their entirety?	2			Reports submitted to IEHP by the 15th of the month due	YES=2; NO=0
B	Were all quarterly reports submitted timely, accurately and completed in their entirety?	1			Reports submitted to IEHP by the last day of the month following the end of the quarter	YES=1; NO=0
C	How many extensions were granted over the year?	1			Extensions are requested before the reporting deadline, for extenuating circumstances only	0-3 Extensions= 1; 4 or more Extensions= 0
D	Did the IPA report whether or not they had any deficiencies throughout the year?	1			The IPA must report even if they had no deficiencies	YES=1; NO=0
3	Claims Appeals –03/11 - 02/12 (4 points)					
A	Did the IPA have any appealed claims?	4			No appealed claims; if appealed claims proceed to 2B.	0 appeals=4; Go to Question 4; Appealed claims=Go to Question 3B
B	If Provider had appealed claims:					
a	What percentage of IPA claims did the IPA fail to respond to IEHP's written request for claims payment or denial information which lead to IEHP having to pay the claim and deduct from the IPA's capitation?	3			Score is equal or less than 24%	100%-75% =0; 74%-50%=1; 49%-25%=2; <24%=3
b	What percentage of all IPA denials were overturned and paid by IEHP?	1		-	Score less than or equal to 10%	0-10%=1; >10%=0
4	Member Claim Bills Activity (Bills received by Members for non-payment or balance due for underpayment) 03/11 - 02/12 (2 points)					
A	Did the IPA have any Member Claim Bill activities?	2			No Member Bills	0 Member Bills=2; Member Bill activity=Go to Question 3Ba
B	If IPA had Member Claim Bill activities:					
a	What percentage of Member Claim Bill cases received did IEHP have to pay and deduct from the IPA's capitation?	1			Score less than or equal to 25%	0-25% =1; <25%=0
CLAIMS POINTS SCORED:		20				

**Inland Empire Health Plan
IPA Performance Evaluation Tool 2011/2012**

FUNCTIONAL AREA		Poss	Score	Scored	IEHP Expectation	IEHP Scoring
II	COMMUNICATION				Total possible points:	5
1	Communication of PCP Changes – 03/11 - 02/12 (2 points)					
A	Does IPA communicate changes in its PCP network in a timely manner and include required information as stated in policy 18.C?	2			Provides 60-day advance notification for all changes	100%-75%=2; 74%-50%=1; <49%=0
2	Quarterly Submission of Specialty Network - 03/11 - 2/12 (2 points)					
A	Does IPA communicate changes in its Specialist network on a quarterly basis in timely, complete manner and including all required information as stated in policy 18.F?	2			Verified network returned by due date specified in quarterly specialty network letter	100% - 75%=2; 74% - 50%=1; <50%=0
3	Recredentiaing Packet Submission - 03/11 - 2/12 (1 point)					
A	Does IPA submit practitioners Recredentiaing packets within 30 days of the IPAs Credentiaing Committee approval including all required information as stated in policy 5.B?	1			Recredentiaing packet received within 30 days of the IPA Credentiaing Committee	100%-80%=1; <80%=0
COMMUNICATION POINTS SCORED:		5				

FUNCTIONAL AREA		Pts Poss	Raw Score	Pts Scored	IEHP Expectation	IEHP Scoring
III	ENCOUNTER DATA				Total possible points:	10
1	Monthly Data Submission – 03/11 - 02/12 (10 points)					
A	Are IPA submissions meeting IEHP validity requirements?	5			See standards outlined in Policy 21A	100%=5; 99%-80%=2; <80%=0
B	Are IPA submissions meeting IEHP adequacy requirements?	5			See standards outlined in Policy 21A	100%=5; 99%-80%=2; <80%=0
ENCOUNTER DATA POINTS SCORED:		10				

Inland Empire Health Plan
IPA Performance Evaluation Tool 2011/2012

FUNCTIONAL AREA		Pts Poss	Raw Score	Pts Scored	IEHP Expectation	IEHP Scoring
IV	FINANCE				Total possible points:	10
1	Financial Viability – Calendar Year 2011 Submissions (10 points)					
A	Does the IPA submit their quarterly financial reports within the required timeframe?	1			Reports submitted to IEHP by the 15th of the month due	100%=1; <100%=0
B	Did the IPA always pass IEHP's quarterly financial viability test the first time?	1			Passed quarterly financial viability test each quarter; no corrective action needed	PASS=1, FAIL=0
C	Did the IPA pass DMHC's quarterly financial viability test each quarter?	2			Passed quarterly financial viability test each quarter; no corrective action needed	PASS=2, FAIL=0
D	Did the IPA submit the 2010 Audited Annual Financial Statement within the required timeframe?	2			Provided as requested by IEHP	YES=2; NO=0
E	Did the IPA pass the 2010 Audited Annual Financial Viability Test?	2			Passed quarterly financial viability test each quarter; no corrective action needed	PASS=2, FAIL=0
F	Did the IPA secure the required Letter of Credit (LOC)?	2			Provided as requested by IEHP	YES=2; NO=0
FINANCE POINTS SCORED:		10				

FUNCTIONAL AREA		Pts Poss	Raw Score	Pts Scored	IEHP Expectation	IEHP Scoring
V	GRIEVANCES				Total possible points:	8
1	Member Grievances (Rec'd by IPA) – 01/11 - 12/11 (3 points)					
A	Are grievance responses received timely from the IPA?	1			Score = 90% received within 14 days	100%-90%=1; <90%=0
B	Upon resolution, how many Grievances were found to be Level 2 and Level 3 (per 1000)?	2			Score < or = IEHP Avg. (IEHP ave +1 std deviation)	< or =2; >=0
2	Member Appeals : 01/11- 12/11 (5 points)					
A	How many Appeals were received (per 1000)?	1			Score < or = IEHP Avg. (IEHP ave +1 std deviation)	< or =1; >=0
B	How many denials were overturned upon appeal (per1000)?	4			Score < or = IEHP Avg. (IEHP ave +1 std deviation)	< or =4; >=0
GRIEVANCES POINTS SCORED:		8				

Inland Empire Health Plan
IPA Performance Evaluation Tool 2011/2012

FUNCTIONAL AREA		Pts Poss	Raw Score	Pts Scored	IEHP Expectation	IEHP Scoring
VI	DELEGATION OVERSIGHT AUDIT RESULTS - 2011				Total possible points:	24
1	Quality Management NCQA (3 points)					
A	Delegation Oversight Audit score:	3			Must score a minimum of 80% to pass audit. Score based upon initial audit score	96-100%=3; 90-95%=2; 80-89%=1; < 79%=0
2	Utilization Management NCQA (3 points)					
A	Delegation Oversight Audit score:	3			Must score a minimum of 80% to pass audit. Score based upon initial audit score	96-100%=3; 90-95%=2; 80-89%=1; < 79%=0
3	Utilization Management Denial File Review (3 points)					
A	Delegation Oversight Audit score:	3			Must score a minimum of 80% to pass audit. Score based upon initial audit score	90-100%=3; 89.99-80%=2; < 80%=0
4	Utilization Management Approved File Review (3 points)					
A	Delegation Oversight Audit score:	3			Must score a minimum of 80% to pass audit. Score based upon initial audit score	90-100%=3; 89.99-80%=2; < 80%=0
5	Credentialing (3 points)					
A	Delegation Oversight Audit score:	3			Must score a minimum of 80% to pass audit. Score based upon initial audit score	96-100%=3; 90-95%=2; 80-89%=1; < 79%=0
6	Care Management (3 points)					
A	Delegation Oversight Audit score:	3			Must score a minimum of 80% to pass audit. Score based upon initial audit score	96-100%=3; 90-95%=2; 80-89%=1; < 79%=0
7	Care Management File Review (3 points)					
A	Delegation Oversight Audit score:	3			Must score a minimum of 80% to pass audit. Score based upon initial audit score	90-100%=3; 89.99-80%=2; < 80%=0
8	Focused Audit (3 points)					
A	Does IPA require a Focused Audit from Delegation Oversight Audit?	3	-		No Focused Audit Necessary	No Audit Necessary=3; Focused Audit=0
DELEGATION OVERSIGHT AUDIT RESULTS PTS SCORED:		24				

**Inland Empire Health Plan
IPA Performance Evaluation Tool 2011/2012**

FUNCTIONAL AREA		Pts Poss	Raw Score	Pts Scored	IEHP Expectation	IEHP Scoring
VII	IPA REPORTING AND MEMBER ACCESS AUDIT				Total possible points:	23
1	Monthly Reports – 01/11 - 12/11 (9 points)					
A	IPA did not require 100% concurrent denial review or focused audit	2			No 100% concurrent denial review or focused audit required.	No concurrent review or focused audit=2; Yes=0
B	Denial decision turnaround time is compliant with guidelines.	2			Complaint with IEHP turnaround timeframes 90% of the time.	100%-90%=2; 89.99-80%=1; < 80%=0
C	IPA utilizes correct denial letter templates?	2			IPA utilizes IEHP approved denial letter templates with correct attachments.	100%-90%=2; 89.99-80%=1; < 80%=0
D	Does IPA submit monthly Care Management and CCS logs that are comprehensive and adhere to IEHP guidelines?	1			Reports adhere to IEHP policy 12.A.3. and are timely and reference all elements.	100%-80%=1; <80%=0
E	Does IPA respond to Care Management/coordination of care calls from IEHP effectively and adhere to IEHP guidelines?	2			Call responses adhere to IEHP policy 12.A.1 (revised/approved UM Subcommittee 5/12/10).	100%-80%=2; <80%=0
2	Annual and Semi Annual Reports - 01/11 - 12/11 (2 points)					
A	Does the IPA submit UM/QM Semi-Annual and Annual Reports that are comprehensive and adhere to IEHP guidelines. (Reports, Program Description, Workplan and Annual Evaluation)	2			Received by IEHP: August 15th (Jan 1- June 30) & February 15th (July 1- Dec 31)	100%-80%=1; <80%=0
3	Member Access 01/11 - 12/11 (12 points)					
A	What percentage of IPA's PCPs passed the Well Child appointment access audit?	3			Score > than or equal to 80%	> or = 90%= 3; 80-89%= 2; < 79%= 0
B	What percentage of IPA's PCPs passed the Routine appointment access audit?	3			Score > than or equal to 80%	> or = 90%= 3; 80-89%= 2; < 79%= 0
C	What percentage of IPA's PCPs passed the Physical appointment audit?	3			Score > than or equal to 80%	> or = 90%= 3; 80-89%= 2; < 79%= 0
D	What percentage of IPA's PCPs passed the Urgent appointment availability audit?	3			Score > than or equal to 80%	> or = 90%= 3; 80-89%= 2; < 79%= 0
IPA REPORTING AND MEMBER ACCESS AUDIT POINTS SCORED:		23				

**Inland Empire Health Plan
IPA Performance Evaluation Tool 2011/2012**

SCORING SUMMARY*

		<u>TOTAL POINTS SCORED</u>		<u>TOTAL POINTS POSSIBLE</u>
1	CLAIMS	0		20
2	COMMUNICATION	0		5
3	ENCOUNTER DATA	0		10
4	FINANCE	0		10
5	GRIEVANCES	0		8
6	DELEGATION OVERSIGHT AUDIT RESULTS	0		24
7	IPA REPORTING AND MEMBER ACCESS AUDIT	0		23
TOTAL POINTS		0		100
TOTAL PERCENTAGE		0%		100%

CONTRACT YEARS AWARDED

Providers achieving the following percentages:

95% or above
85% to 94.99%
80% to 84.99%
Less than 80%

Are awarded a contract term of:

3 years
2 years
1 year
Non-renewal

**Any functional area not reviewed in the PET timeframe will not be included as part of the total score*



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 | <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"/> Othe |

Name: _____

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 potentially fraudulent activity (attach extra sheet, if necessary):

Law Enforcement has been contacted? Yes No

Date Reported: _____ Report Number: _____

Contact Information: _____

State Regulatory Agency has been contacted: Yes No

Date Reported: _____ Report Number: _____

Contact Information: _____

IEHP Case Number: _____

PIU Case Number: _____

Attachment B

BREACH / INCIDENT REPORT



DIRECTIONS: Type answers in the field below each question; type or select 'yes' in the field to the right of each question, whenever applicable (in multiple cells to a single section, if necessary). For section 16, please refer to 'HITECH Breach Definitions and Exceptions' link provided.

The information in this report will be used, in part, to determine whether a breach has occurred.

Please continue to check DHCS website for most updated version of Breach / Incident

* = Required items within 72 hours of discovery, to the extent known

† = Health and Human Services (HHS) required information

Please specify whether: Notice to DHCS, Investigation Report, Complete Report, or Supplemental Report from drop-down menu to the right. ---

1. SUMMARY OF BREACH / INCIDENT * † (Please include location of the breach / incident, how the breach / incident occurred, and any information regarding the type of media and protected health information involved in the breach / incident.)

(type Summary of Breach / Incident here; cell will expand to accommodate 1000 characters; attach separate sheet if necessary.)

2. BASIC INFORMATION * †

DHCS Breach / Incident Number:

(type DHCS Breach / Incident Number here)

Reporting Entity's Breach/Incident Case Number

(type Reporting Entity's Breach/Incident Case Number here)

Date of Most Recent Update (Today's Date); Please Highlight All New or Changed Information

(MM/DD/YYYY)

Reporting Entity:

(type Reporting Entity here)

Entity That Caused Breach / Incident:

(type Breaching Entity here)

Date(s) of Incident / Breach:

(MM/DD/YYYY)

Date(s) of Discovery:

(MM/DD/YYYY)

Date of Notice to DHCS:

(MM/DD/YYYY)

Approximate Number of Individuals Affected by Breach / Incident:

(type Approximate Number of Individuals Affected by Incident / Breach here)

What was the primary job function of the person(s) known, or reasonably believed, to have improperly sent, used, accessed, or disclosed PHI/PI (include employer, employee status, and any other pertinent information).

(describe job functions of person(s) here; cell will expand to accommodate text)

What was the primary job function of the person(s) who viewed or (accidentally) obtained PHI/PI (include employer, employee status, and any other pertinent information).

(describe job functions of person(s) here; cell will expand to accommodate text)

3. CONTACT INFORMATION * †	
Attention:	
(type Attn here)	
Street:	
(type Street here)	
City:	
(type City here)	
State:	
(type State here)	
Zip Code:	
(type Zip Code here)	
Reporting Entity's Contact's Name	
(type Reporting Entity's Contact's Name here)	
Reporting Entity's Contact's Email	
(type Reporting Entity's Contact's Email here)	
Reporting Entity's Contact's Number	
(XXX-XXX-XXXX)	
Privacy / Compliance Officer:	
(type Privacy / Compliance Officer here)	
Privacy / Compliance Officer's Email:	
(type Privacy / Compliance Officer's Email here)	
Privacy / Compliance Officer's Phone Number:	
(XXX-XXX-XXXX)	
List contact information of any other entities and/or person(s) that breach / incident was reported to:	
(type contact information here; cell will expand to accommodate text.)	
4. PROTECTED HEALTH INFORMATION (PHI) *	Type or select 'yes' from drop-down menu.
Does the information disclosed in the breach / incident provide a reasonable basis to believe it can be used to identify an individual?	

Does the information disclosed in the breach / incident relate to the past, present, or future physical or mental health, or condition of an individual?	

Does the information disclosed in the breach / incident relate to the provision of health care to an individual?	

Does the information involved in the breach / incident relate to the payment or provision of health care to an individual?	

5. TYPE OF ENTITY * †	Type or select 'yes' from drop-down menu.
Health Plan	

Health Care Provider	

Health Care Clearinghouse	

Other (please explain function and involvement in breach)	

(if other, please explain function and involvement in breach here; cell will expand to accommodate text)	
6. TYPE OF BREACH / INCIDENT * †	Type or select 'yes' from drop-down menu.
Theft	

Loss	

Improper Disposal	

Unauthorized Access	

Unauthorized Disclosure	

Exhibit ___
HIPAA BUSINESS ASSOCIATE ADDENDUM

<i>Mis-Sent</i>	---
<i>Hacking/IT incident</i>	---
<i>Unknown</i>	---
<i>Other (explain)</i>	---
(if other, type explanation here; cell with expand to accommodate text)	
7. TYPE OF PROTECTED INFORMATION INVOLVED IN THE BREACH / INCIDENT * †	Type or select 'yes' from drop-down menu.
DEMOGRAPHIC INFORMATION	
<i>First Name (or Initial)</i>	---
<i>Last Name</i>	---
<i>Address/Zip</i>	---
<i>Date of Birth</i>	---
<i>SSN</i>	---
<i>Drivers License</i>	---
<i>Other Identifier</i>	---
FINANCIAL INFORMATION	
<i>Credit Card/Bank Acct #</i>	---
<i>Claims Information</i>	---
<i>Other Financial Information</i>	---
CLINICAL INFORMATION	
<i>Diagnosis/Conditions</i>	---
<i>Medications</i>	---
<i>Lab Results</i>	---
<i>Other Treatment Information</i>	---
OTHER (explain)	---
(if other, type explanation here; cell will expand to accommodate text)	
<i>Of the data elements in Section 7, were any provided to you by DHCS?</i>	---
8. LOCATION OF INFORMATION DISCLOSED IN BREACH OR INCIDENT * †	Type or select 'yes' from drop-down menu.
<i>Laptop</i>	---
<i>Desktop Computer</i>	---
<i>Network Server</i>	---
<i>Email</i>	---
<i>Other Portable Electronic Device</i>	---
<i>Electronic Medical Record</i>	---
<i>Paper Data</i>	---
<i>Blackberry</i>	---
<i>Cell phone</i>	---
<i>Hard Drive (External)</i>	---
<i>Hard Drive (Internal)</i>	---
<i>CD/DVD</i>	---
<i>PDA</i>	---
<i>Tape/DLT/DASD</i>	---
<i>USB Thumb Drive</i>	---
<i>Other (explain)</i>	---
(if other, type explanation here; cell will expand to accommodate text)	
9. SAFEGUARDS IN PLACE PRIOR TO BREACH / INCIDENT †	Type or select 'yes' from drop-down menu.
<i>Firewalls</i>	---

Exhibit ___
HIPAA BUSINESS ASSOCIATE ADDENDUM

<i>Packet Filtering (router-based)</i>	---
<i>Secure Browser Sessions</i>	---
<i>Strong Authentication</i>	---
<i>Encrypted Wireless</i>	---
<i>Physical Security</i>	---
<i>Logical Access Control</i>	---
<i>Anti-virus Software</i>	---
<i>Intrusion Detection</i>	---
<i>Biometrics</i>	---
<i>Was staff involved in breach trained in HIPAA Privacy Security within the past year?</i>	---
10. MALICIOUS CODE / MALWARE TYPE	Type or select 'yes' from drop-down menu.
<i>Worm</i>	---
<i>Virus</i>	---
<i>Trojan</i>	---
<i>Buffer Overflow</i>	---
<i>Denial Service (DoS)</i>	---
<i>Other (explain)</i>	---
<i>(if other, type explanation here; cell will expand to accommodate text)</i>	
11. ACTIONS TAKEN IN RESPONSE TO BREACH / INCIDENT †	Type or select 'yes' from drop-down menu.
<i>Security and/or Privacy Safeguards</i>	---
<i>Mitigation</i>	---
<i>Sanctions</i>	---
<i>Policies and Procedures</i>	---
<i>Other (explain)</i>	---
<i>(if other, type explanation here; cell will expand to accommodate text)</i>	
12. DATA AND RECOVERY *	Type or select 'yes' from drop-down menu.
<i>Were any DHCS systems involved?</i>	---
<i>Was the data recovered?</i>	---
<i>If data was recovered, specify what, when, and who has it now.</i>	
<i>(if data was recovered, type explanation here; cell will expand to accommodate text)</i>	
<i>If not recovered, explain: (still missing / shredded / under investigation)</i>	
<i>(if not recovered, type answer here; cell will expand to accommodate text)</i>	
<i>Impact of Incident - potential misuse of data, identity theft, etc.</i>	
<i>(describe impact of incident here; cell will expand to accommodate text)</i>	
13. MEDI-CAL DATA	Type or select 'yes' from drop-down menu.
<i>How many Medi-Cal beneficiaries' PHI or PI were impacted by the breach/incident?*</i>	
<i>(type number of Medi-Cal beneficiaries here)</i>	
<i>Children (< 18 yrs.) Medi-Cal beneficiaries data breached?</i>	---
<i>Was PHI or PI in question utilized in the administration of the Medi-Cal Program?</i>	---
<i>Was Client Index Number (CIN) breached?</i>	---
14. SUPPLEMENTARY DESCRIPTION OF BREACH / INCIDENT † (Please include any supplementary information regarding the location of the breach, how the breach occurred, and the type of media and protected health information involved in the breach.)	
<i>(type supplementary description here; cell will expand to accommodate 1000 characters; attach separate sheet if necessary)</i>	

Exhibit ___
HIPAA BUSINESS ASSOCIATE ADDENDUM

15. CORRECTIVE ACTION, MITIGATION, NOTIFICATION, AND INVESTIGATION	Type or select 'yes' from drop-down menu.
<i>Describe Corrective Action Plan and Status (attach CAP separately if needed)</i>	
(type Corrective Action Plan and Status here; cell will expand to accommodate 1000 characters; attach separate sheet if necessary)	
<i>Was Corrective Action Plan approved by DHCS?</i>	---
<i>Describe Mitigation Plan and Status (attach Mitigation Plan separately if needed)</i>	
(type Mitigation Plan and Status here; cell will expand to accommodate 1000 characters; attach separate sheet if necessary)	
<i>Investigation Status (i.e. completed, estimated completion date, etc.)</i>	
(type Investigation Status here; cell will expand to accommodate text)	
<i>Breach Notification Letter Status (also, specify if approved by OHC)</i>	
(type Breach Notification Letter Status here; cell will expand to accommodate text)	
<i>Individual Notification Sent By</i>	
(type who sent Individual Notification here; cell will expand to accommodate text)	
<i>Date Sent</i>	
(MMDDYYYY)	
16. HITECH - BREACH DEFINITIONS AND EXCEPTIONS * (Please refer to link below and select 'Definition of a Breach' for reference)	Type or select 'yes' from drop-down menu.
<i>link: HITECH Breach Definitions and Exceptions</i>	
<i>Did incident fall under one of the three breach exceptions? (Please refer to link above and select 'Definition of a Breach' for reference.)</i>	---
(If incident fell under one of the three breach exceptions, please explain circumstances here.)	
Please return form to: privacyofficer@dhs.ca.gov or fax to: (916) 440-7680	

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

Attachment 23-5 - DHHS PB Notification Form Affecting 500 or More Individuals

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



("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 Attachment 23-5 - DHHS PB Notification Form Affecting 500 or More Individuals
 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 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

Attachment 23-6 - DHHS PB Notification Form Affecting Less Than 500 Individuals

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

("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 Attachment 23-6 - DHHS PB Notification Form Affecting Less Than 500 Individuals
 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