DEPT. COMM. NO. 74

LINDA LINGLE
GOVERNOR OF HAWAII

CHIYOME L. FUKINO, M.D.
DIRECTOR OF HEALTH

STATE OF HAWAII
DEPARTMENT OF HEALTH
P.O. Box 3378
HONOLULU, HAWAII 96801-3378

In reply, please refer to:
File:

February 18, 2010

The Honorable Colleen Hanabusa, President
Member of the Senate
Twenty-Fifth State Legislature
State Capitol, Room 409
Honolulu, Hawaii 96813

Dear Senator Hanabusa:

Attached is the legislative report and other relevant documents as required by HRS 487N and Department of Health (DOH) Privacy Policy 26.01. This notification is being sent to you as a result of a Security Breach that occurred on January 13, 2010 by a Case Management Unit of the Developmental Disabilities Division.

The DOH shall provide more follow-up information should any new developments occur. If you have any questions, please contact Dr. David Fray, Chief of Developmental Disabilities Division, at 586-5842.

Sincerely,

Chiyome Leinaala Fukino, M.D.
Director of Health

Attachments

Report to the Legislature
Department of Health
Developmental Disabilities Division
Security Breach

DEPT. COMM. NO. 74

Summary

On Wednesday, January 13, 2010, Case Management Unit 8 of the Developmental Disabilities Division (DDD) was scheduled to move from Hale F across the courtyard to Hale D on the Pearl City, Waimano campus, among other Unit offices. In the course of the move, a 2-drawer metal file cabinet belonging to one Case Manager from Unit 8 did not arrive at the new office space. After checking with the movers and searching the Waimano campus, it was determined that the file cabinet was missing. Subsequently, Unit 8's supervisor reported the incident to the Honolulu Police Department, who opened an investigation.

The Case Manager is unsure what documents the file cabinet may contain, as she does not use it often. It is clear, due to extensive checking, that client files were not contained in the missing file cabinet. To the best of her knowledge, the file cabinet may contain approximately two client intake sheets, of which she was the intake worker. Checking against DDD's database, both intake sheets contained protected health information as defined by the HIPAA Privacy Rule (Health Insurance Portability and Accountability Act of 1996); and one of the two the intake sheets also included the social security number of that applicant, triggering Hawaii Revised Statutes Chapter 487N.

On February 4, 2010, the Governor via her Chief of Staff, Senior Policy Advisor and Chief of Media Relations were sent a memo informing them of this incident. In addition, the two individuals potentially affected by this incident were properly notified as per requirements by the HIPAA Privacy Rule and HRS Chapter 487N on that date.

Detailed Information Relating to the Nature of the Breach

Please refer to attached Timeline Regarding Missing File Cabinet.

Number of Individuals Affected & Notified

Due to careful cross-checking of documents and databases, it was determined that two individuals may be potentially affected by this incident. And while the Case Manager is unable to say with any certainty that a client's social security number or any other protected health information under HIPAA was kept in the missing file cabinet; in consideration of the public trust and the Department's commitment to safeguarding the information entrusted to us, the Department shall treat this incident as a security breach.

To date, both individuals have been sent notice of the potential breach of their protected health information. *A copy of these notification letters is attached to this report.*

Corrective Action Plan

The Corrective Action Plan has identified five activities that will prevent a breach like this from occurring again. This includes the following:

- Case management staff will schedule 2 hours per month to shred and/or purge unnecessary PHI from desks and file cabinets.
- Case management staff will review DOH HIPAA Policy P03.01- Minimum Necessary to ensure that staff learns to "limit the use, disclosure or request of PHI to the minimum necessary amount need to accomplish the intended task".
- DDD forms committee will review the PHI elements contained on current DDD forms to identify unnecessary PHI and make recommendations for revision.
- Case management staff will ensure that documents are not kept/transported when a case manager leaves one unit and joins another.
- Case management staff will review memo regarding moving suggestions to track items transported during a move.

See attached Corrective Action Plan (CAP) for more details.

TIME LINE REGARDING MISSING FILE CABINENT

February 4, 2010

Affected Office:

Case Management Unit 8
2201 Waimano Home Road
Pearl City, Hawaii 96782
Phone: 453-5985

Description of what happened per interview with Unit Supervisor, Case Manager (CM), and DDD HIPAA Privacy Coordinator.

Note: Information related to the discovery of the type and amount of missing PHI is bolded and italicized.

Wednesday, January 13, 2010:

8:30 to 11:30 AM:
Case Management Unit 8 (CMU 8) office relocated from Hale F to Hale D on the Waimano Complex Campus of the Developmental Disabilities Division. OCCC had been contracted by the Case Management and Information Services Branch (CMISB) to assist with all moves in the month of January 2010. There were approximately 6 inmates that worked as movers that morning. Their supervisor was present at all times.

8:45 AM: Case Manager (CM) arrived from field visits to the new office located at Hale D. She surveyed that all of her boxes, cabinets, computer, and desk were accounted for. However, she noticed that a 2-drawer, beige, vertical filing cabinet was missing. This cabinet had been taped shut and had her name or her initials written in permanent marker on the front of this beige cabinet by the lock. The cabinet has a lock, CM has a key, but she was not sure if she locked it prior to the move or not. CM reported the last time she was able to account for cabinet was at 3:15 PM on 01/12/2010. ***Per CM, this particular cabinet was not utilized routinely except to store her purse during the day when she was at work and to put her personal personnel records and resource files within. CM. also stressed that all of her client DOH folders are in the secure designated cabinet. Her folders utilized for field visits were also secured and accounted for.***

Within minutes of the discovery she asked the movers where the cabinet was and was told by the moving supervisor that the file should be somewhere at Building D, but he did not know where her specific two drawer was but would look out for it. She then waited for the contents of the other co-workers to be moved, hoping her cabinet would show up. She again asked the moving supervisor and he said he didn't know. She questioned if anything had been placed in the truck and was told, "Nothing has been removed or would be removed from this building or complex".

It was noted by the Unit Supervisor that the CM was provided instructions regarding how to prepare for the move. However, an emergency situation with a client had occurred and the Unit Supervisor is unsure if she was able to prepare as advised. Label tags were provided and the CM used tags for most of her contents but unsure if tag was fastened to the file cabinet.

The CM began looking in other cubicles to find her cabinet. The Unit Supervisor looked also in Hale F, the office from which CMU 8 had moved to no avail. The Unit Supervisor informed all of the staff at CMU 8 to watch out for the cabinet, providing a description. She also informed the CMU 5 supervisor, CMU 7 supervisor, and the staff present to help keep an eye out for the cabinet. The West Oahu Section Supervisor was also notified. She and her Secretary were moving in to the Hale F Building. The CM's supervisor also informed the Case Management and Information Services Branch (CMISB) Branch Chief of the missing cabinet. The Branch Chief was present for the move as well as a meeting scheduled in Hale C. CMU 6, who occupy the other wing of Hale D were also notified. The Unit Supervisor also mentioned it to other clerical and supervisory staff to keep an eye open for it. Other staff visiting the Waimano Complex that day included the Contracts and Resource and Development Section (CRDS) Supervisor who was meeting with the CMISB Branch Chief at Hale C. The Opportunities for the Retarded, Inc. (ORI) Cleaning Team was also present on campus that day.

Later that day, the Unit Supervisor emailed all supervisors at the Waimano complex, including the Direct Services Branch Staff, located in Building A, and the Personnel office located in Hale B, to look out for the cabinet. Per the Unit Supervisor, she had not heard that any other office contents are missing.

The CM also went to the occupied Hale Buildings and asked all staff to look out for her 2 drawer cabinet.

The overall consensus of all was that the cabinet had to be on campus somewhere. It was heavy and not easily moved. Staff felt confident that it could be found.

Thursday, January 14, 2010:

The search of the cabinet continued. The CM asked for the assistance of the Direct Services Branch Chief, to open Hale C to search for the cabinet. No success.

The Unit Supervisor informed East Oahu Section Supervisor. The East Oahu Section Supervisor also spoke with the CM. All remained confident that the cabinet would shortly be found somewhere on the campus.

Tuesday, January 14, 2010:

A Tri-Sectional meeting was held at the Pearl City State Lab. The CMISB Branch Chief made an announcement at the beginning of the meeting for all Oahu case management units and supervisors about the missing file cabinet and to look out for it.

Other moves on the Waimano Campus were continuing that week and the overall hope of all was that the cabinet would most likely turn up after all offices were settled. The search was to continue for the cabinet.

It was noted that no other items, cabinets, or other furniture was missing from the moves conducted thus far.

Tuesday, January 26, 2010:

A CORE meeting of supervisors was held at Diamond Head Health Center. During this meeting, The DDD HIPAA Privacy Coordinator presented the HIPAA Policy 04.13. Following the meeting, the Unit Supervisor spoke with the HIPAA Privacy Coordinator, about the missing file cabinet. ***The concern was that the Case Manager's private personnel information might be considered HIPAA; her understanding based on discussions with the CM was that the cabinet contained only personal information. The HIPAA Privacy Coordinator explained that she would contact the HIPAA office, but her understanding that as it was the case manager's personal information that it would not be a HIPAA violation for the Division.*** She advised that the CM act quickly to protect herself by calling credit reporting agencies as soon as possible. The HIPAA Privacy Coordinator shared that she would talk to the DOH HIPAA office for clarification. The HIPAA Privacy Coordinator met with the DOH HIPAA office later that day. After conferring about the cabinet they agreed that it was not a HIPAA concern and recommended she contact the three credit reporting agencies to alert them of possible stolen protected health information. The HIPAA Privacy Coordinator sent the CM an email reflecting their recommendations.

Thursday, January 28, 2010:

The HIPAA Privacy Coordinator met with the CM regarding another unrelated event. ***The topic of the missing file cabinet came up and the HIPAA Privacy Coordinator asked her again regarding the content of the file cabinet. She stated that she could not guarantee that there was no client information in cabinet. She stated she wasn't sure what was in the cabinet.*** The HIPAA Privacy Coordinator then reported this to the HIPAA office that it was possible that the cabinet contained client PHI. The HIPAA office advised the HIPAA Privacy Coordinator to ensure that the campus was searched again thoroughly by the end of the day. Friday was a furlough day.

The Unit Supervisor was not present on campus on Thursday, 1/28/2010. The CM enlisted the support of the CMU 7 supervisor; they went to each building and cooperatively conducted a through search of all buildings and offices with no success.

Monday, February 1, 2010:

The HIPAA Privacy Coordinator emailed and later spoke with the Unit Supervisor requesting that she speak further with CM about the file cabinet and explained that the type of information will determine the type of remediation. The CM was out of the office and her supervisor assured the HIPAA Privacy Coordinator that she would contact her.

Later that day, The HIPAA Privacy Coordinator was called and emailed by the Unit Supervisor to share that CM continued to explain that she could not recall the complete contents of the cabinet. She could not say without certainty that the file did not contain client information. The CM noted that the file might have contained client lists and completed intake forms. The HIPAA Privacy Coordinator advised the Unit Supervisor to work with the CM to complete the Privacy Incident Report Form as soon as possible.

That same day, the Unit Supervisor and the Direct Services Branch Chief, conducted a thorough search of the campus. During this search each office was checked and cabinets matching the description were opened with the permission of the staff to check for contents. Hale A, B, C, D, E, and F were all searched with no success.

February 2, 2010, Tuesday:

The DOH HIPAA office, met with HIPAA Privacy Coordinator to conference call the CM to further determine and discuss the elements of the records that may have been in the file cabinet and timeline. ***The HIPAA Office and the HIPAA Privacy Coordinator spoke with the CM and Unit Supervisor and it was shared by the CM that a client list from the DDCares System might be in the cabinet. This list includes the full name of the client, the Social Security Number, Birthdates, and who was assigned. This would include 308 client names and that she might also have a list from when she worked at CMU 5 (she was employed there from 2002-2008). She also explained that there may be intake forms that include SSN, Address, Phone, Birthdate and Full Name. She noted she may have approximately 100 of those in her file.***

Because of the nature of the contents, the HIPAA office quickly notified the DDD Chief who in turn notified the designated Attorney General (who had been previously notified) that the contents may *now* potentially included SSN which could put clients at financial risk. The DDD Chief then notified the Deputy Director of Behavioral Health Administration and Deputy Director of Health. The DDD Chief also advised that they police should be called to make a police report.

Later that afternoon, the DDD Chief spoke with the CM who had since had an opportunity to start a more intensive search of her client files and lists.

February 3, 2010:

11:30 AM: The Unit Supervisor went to the Police Department located at 1101 Waimano Home Road in Pearl City and submitted a police report regarding the missing cabinet. Summarizing incident and agreeing to prosecution.

Report Number: 10-042922
Officer: K. Capellas
Theft, 3rd degree

1:00 PM: ***Consultation with the CM who shared that she has ascertained that all client listings are accounted for, client charts, and working folders all in secure cabinets' in her office.***

The CM had narrowed the concern to intake cases within CMU 8. She had already communicated with the DDD Chief, on the afternoon of February 2, 2010.

3:30 PM: Telephone call from the HIPAA Privacy Coordinator requesting listing of potentially affected clients. Unit Supervisor shared that the CM had left for the day, but would gather a listing of all intake cases which the CM had worked on from the time she became employed by CMU 8 in 09/2008 to 01/2010 and then have the CM review the list with her existing secure records when she came in on 2/4/2010.

4:15 PM: ***Following a review of the intake listing the CM had been assigned 16 cases during the period of 09/2008 to 01/2010. Information verbally provided to HIPAA Privacy Coordinator.*** The HIPAA Privacy Coordinator requested that the information be faxed to the Division office so that letters could be generated to the affected individuals. The Unit Supervisor shared that she would do so following a review by the CM the following morning.

February 4, 2010:

8:00 AM: ***The CM reported to her supervisor that she had reviewed the listing of intake clients and were able to account for all intake information except for 2 clients that she could not find information on.*** The Unit Supervisor requested that this information be faxed to Division, including client name and address so they could be properly notified.

The CM stressed that she did not know for certain that this information was in the cabinet. The only content she knows with conviction was in the cabinet was her own personal personnel information and some resource files.

The search for this cabinet will continue, however, through searches of the Waimano Campus has occurred on multiple occasions without success.

3:00 PM: ***In the process of preparing the letters to the affected clients, it was determined that one of the clients had not provided a social security number at intake reflected in the DD Cares Client Profile that had been generated from during the intake process.*** The letter to this individual was changed to ensure that the possible missing information did not include his/her social security number. The letters were mailed later that day. In addition, the letters to the Governor's office were routed through the Deputy Director of Behavioral Health, Deputy Director of Health and the Director of Health's office for approval. DDD Chief delivered the approved letters to the Governor's office. Copies of the letters to the Governor and to the affected clients will be provided to the HIPAA office on Monday, February 8.

LINDA LINGLE
GOVERNOR OF HAWAII

CHIYOME LEINAALA FUKINO, M.D.
DIRECTOR OF HEALTH

STATE OF HAWAII
DEPARTMENT OF HEALTH
DEVELOPMENTAL DISABILITIES DIVISION

PO BOX 3378
HONOLULU, HAWAII 96801
TELEPHONE (808) 586-5840
FAX NUMBER (808) 586-5844

In reply, please refer to:
File:

February 4, 2010

Dear Client #1,

This letter is to inform you of a possible security breach with the Developmental Disabilities Division (DDD) that may have involved some of your personal records or information.

The DDD recently became aware of a potential security breach at our Waimano campus site. On Wednesday, January 13, 2010, a routine office move was scheduled from one building to another within the Waimano site. During this move, a two-drawer metal filing cabinet of a case manager went missing. The case manager immediately reported this incident to the area supervisor.

The Department of Health places great value in the public's trust and we are committed to safeguarding the information entrusted to us; therefore, even though the case manager using the missing filing cabinet is unsure if any client information was in there, we are treating this incident as a worst-case scenario.

Based upon an extensive check of files, charts and documents, if the filing cabinet did contain client information, it is most likely limited to intake forms the case manager completed. You are receiving this letter because your intake sheet was identified as one that may have been stored in the missing file cabinet. The information routinely collected on the intake forms includes, but is not limited to the following: the individual's full name, address, telephone number, date of birth, Social Security Number, and the name, address and telephone number of the individual's parent or guardian. In your case, your Social Security Number was not included.

To protect you from the possibility of identity theft, we recommend you place a fraud alert on your credit files. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit reporting agencies at a number below. As soon as one agency confirms your fraud alert, the others will be notified to place similar fraud alerts. You will then be eligible to receive free credit reports from each of the credit reporting agencies.

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

www.equifax.com www.experian.com www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts you did not open or inquiries from creditors you did not initiate. Also, look for personal information like home address and Social Security number that is not accurate. If you see anything that you do not understand, call the credit reporting agency at the telephone number above.

If you find suspicious activity on your credit reports, call your local police department and file a report of identity theft. We suggest you obtain a copy of the police report for your file; you may need to provide copies of the report to creditors to absolve you of fraudulent debts. You may also consider filing a compliant with the Federal Trade Commission at www.consumer.gov/idtheft/ or at 1-877-ID-THEFT (438-4338). Your complaint helps law enforcement officials across the country in their investigations.

If you find your credit card account(s) were affected, we suggest you immediately close them. Consult with your financial institutions about whether to close bank or brokerage accounts, or change your passwords and have the institution monitor for possible fraud. When placing passwords on new accounts avoid using your mother's maiden name, your birth date, the last four digits of your Social Security number, your telephone number, or a series of consecutive numbers for better security.

If you are a victim of identity theft, you also have the option of placing a free security freeze on your credit reports. A security freeze stops consumer credit reporting agencies from releasing any information to unauthorized parties without your express authorization. To request a security freeze on your credit reports, submit your request in writing by certified mail to all three credit reporting agencies at the addresses below along with a copy of a police report, investigative report, or complaint you filed with a law enforcement agency about the unlawful use of your personal information. The agencies will then send you a written confirmation of the security freeze along with a unique personal identification number or password to be used by you to lift the freeze.

Equifax	Experian	TransUnion
Security Freeze	Security Freeze	To request a Security Freeze
P.O. Box 105788	P.O. Box 9554	Form, call: 1-888-909-8872
Atlanta, GA 30348	Allen, TX 75013	

Even if you find no suspicious activity on your initial credit reports, we recommend you continue checking periodically. Federal law entitles you to one free credit report (at your request) once every 12 months from the three nationwide credit reporting agencies listed above. Thus, we recommend you request a free copy of your credit

report from a different agency every four months. This will provide you with three opportunities in a 12-month period to review your credit report for free.

The unauthorized access of your personal information may not result in any harm to your credit reputation or to your personal finances. However, your information which may be accessed could be used for illegal purposes. To protect against that possibility, we advise you to take the steps outlined above. Helpful websites include www.hawaii.gov/dcca/quicklinks/id_theft_infor/ and the previously mentioned www.consumer.gov/idtheft/.

We very much regret this incident occurred and the impact it may have on you. We are continuing to look for the missing file cabinet and have filed a police report. This matter is currently being investigated. It is our hope to find the missing file cabinet soon with all the documents secured inside.

To ensure this type of incident does not occur again, we are reviewing our current privacy and security policies and procedures to find areas where improvements are needed and make corrections. This may include, but is not limited to: a regular removal/shredding of out-dated client information from staff files, removal of unnecessary social security numbers from forms, and procedures to track items transported during a move.

If you have any questions, would like further information about this incident, or need any assistance, please call me at 586-5842.

Sincerely,

David F. Fray
Chief, Developmental Disabilities Division

LINDA LINGLE
GOVERNOR OF HAWAII

CHIYOME LEINAALA FUKINO, M.D.
DIRECTOR OF HEALTH

STATE OF HAWAII
DEPARTMENT OF HEALTH
DEVELOPMENTAL DISABILITIES DIVISION

PO BOX 3378
HONOLULU, HAWAII 96801
TELEPHONE (808) 586-5840
FAX NUMBER (808) 586-5844

In reply, please refer to:
File:

February 4, 2010

Dear Client #2:

This letter is to inform you of a possible security breach with the Developmental Disabilities Division (DDD) that may have involved some of XXX personal records or information.

The DDD recently became aware of a potential security breach at our Waimano campus site. On Wednesday, January 13, 2010, a routine office move was scheduled from one building to another within the Waimano site. During this move, a two-drawer metal filing cabinet of a case manager went missing. The case manager immediately reported this incident to the area supervisor.

The Department of Health places great value in the public's trust and we are committed to safeguarding the information entrusted to us; therefore, even though the case manager using the missing filing cabinet is unsure if any client information was in there, we are treating this incident as a worst-case scenario.

Based upon an extensive check of files, charts and documents, if the filing cabinet did contain client information, it is most likely limited to intake forms the case manager completed. You are receiving this letter because XXX intake sheet was identified as one that may have been stored in the missing file cabinet. The information routinely collected on the intake forms includes, but is not limited to the following: the individual's full name, address, telephone number, date of birth, Social Security Number, and the name, address and telephone number of the individual's parent or guardian.

To protect XXX and yourself from the possibility of identity theft, we recommend you place a fraud alert on her/your credit files. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit reporting agencies at a number below. As soon as one agency confirms her/your fraud alert, the others will be notified to place similar fraud alerts. You will then be eligible to receive free credit reports from each of the credit reporting agencies.

Equifax	Experian	TransUnion
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts you did not open or inquiries from creditors you did not initiate. Also, look for personal information like home address and Social Security number that is not accurate. If you see anything that you do not understand, call the credit reporting agency at the telephone number above.

If you find suspicious activity on your credit reports, call your local police department and file a report of identity theft. We suggest you obtain a copy of the police report for your file; you may need to provide copies of the report to creditors to absolve you of fraudulent debts. You may also consider filing a compliant with the Federal Trade Commission at www.consumer.gov/idtheft/ or at 1-877-ID-THEFT (438-4338). Your complaint helps law enforcement officials across the country in their investigations.

If you find your credit card account(s) were affected, we suggest you immediately close them. Consult with your financial institutions about whether to close bank or brokerage accounts, or change your passwords and have the institution monitor for possible fraud. When placing passwords on new accounts avoid using your mother's maiden name, your birth date, the last four digits of your Social Security number, your telephone number, or a series of consecutive numbers for better security.

If you are a victim of identity theft, you also have the option of placing a free security freeze on your credit reports. A security freeze stops consumer credit reporting agencies from releasing any information to unauthorized parties without your express authorization. To request a security freeze on your credit reports, submit your request in writing by certified mail to all three credit reporting agencies at the addresses below along with a copy of a police report, investigative report, or complaint you filed with a law enforcement agency about the unlawful use of your personal information. The agencies will then send you a written confirmation of the security freeze along with a unique personal identification number or password to be used by you to lift the freeze.

Equifax	Experian	TransUnion
Security Freeze	Security Freeze	To request a Security Freeze
P.O. Box 105788	P.O. Box 9554	Form, call: 1-888-909-8872
Atlanta, GA 30348	Allen, TX 75013	

Even if you find no suspicious activity on your initial credit reports, we recommend you continue checking periodically. Federal law entitles you to one free credit report (at your request) once every 12 months from the three nationwide credit reporting agencies listed above. Thus, we recommend you request a free copy of your credit report from a different agency every four months. This will provide you with three opportunities in a 12-month period to review your credit report for free.

The unauthorized access of your personal information may not result in any harm to your credit reputation or to your personal finances. However, your information which may be accessed could be used for illegal purposes. To protect against that possibility, we advise you to take the steps outlined above. Helpful websites include www.hawaii.gov/dcca/quicklinks/id_theft_infor/ and the previously mentioned www.consumer.gov/idtheft/.

We very much regret this incident occurred and the impact it may have on you. We are continuing to look for the missing file cabinet and have filed a police report and this matter is currently being investigated. It is our hope to find the missing file cabinet soon with all the documents secured inside.

To ensure this type of incident does not occur again, we are reviewing our current privacy and security policies and procedures to find areas where improvements are needed and make corrections. This may include, but is not limited to: a regular removal/shredding of out-dated client information from staff files, removal of unnecessary social security numbers from forms, and procedures to track items transported during a move.

If you have any questions, would like further information about this incident, or need any assistance, please call me at 586-5842.

Sincerely,

David F. Fray
Chief, Developmental Disabilities Division

State of Hawaii Department of Health
Corrective Action Plan (CAP) Form

Instructions: Use this form to submit your **Corrective Action Plan** to the DOH HIPAA Office within thirty days after receipt of a complaint or discovery of a privacy incident (or sooner).

A. Identify the specific area(s) that need improvement to prevent this type of complaint or incident from reoccurring.	B. Describe the corresponding new procedure(s) and/or activities that are being developed and implemented to prevent this type of complaint or incident from reoccurring.	C. Provide a timeline indicating when your program intends to have the new procedure(s) and/or activities fully implemented.	D. List the specific measures that you will use to track and evaluate your progress.
1. CMISB staff will shred and/or purge unnecessary PHI regularly.	Every other month, on the last Monday of each month, staff will be given 2 hours time to shred/purge desks and file cabinets to ensure that unnecessary PHI is left in drawers or cabinets.	This will be done the last Monday of every other month starting in February to ensure old information is not needlessly saved or stored in cabinets and/or drawers.	1. Each Case Management Unit (CMU) will schedule a purge/shred time for their unit in which Case Managers will not be expected to be out in the field or working on other case management duties. 2. Each Case Manager will examine all file cabinets and desk drawers to purge/shred PHI that is no longer needed.
2. CMISB staff will ensure that unit documents are not kept/transported when a Case Manager leaves one unit and joins another.	Unit supervisors to ensure that employees do not take any PHI to another unit/position if they should leave their current position.	A memo will be developed for all employees regarding this issue by February 28, 2010.	1. Memo will be shared with supervisors at joint Unit Head meeting scheduled March 4, 2010. Agenda will document those in attendance. Supervisors will share with unit staff. 2. Supervisor to ask each employee, upon departure from the unit/department/division to return any PHI for that unit

A. Identify the specific area(s) that need improvement to prevent this type of complaint or incident from reoccurring.	B. Describe the corresponding new procedure(s) and/or activities that are being developed and implemented to prevent this type of complaint or incident from reoccurring.	C. Provide a timeline indicating when your program intends to have the new procedure(s) and/or activities fully implemented.	D. List the specific measures that you will use to track and evaluate your progress.
			(lists, etc)
3. CMISB staff will review memo regarding moving suggestions to ensure contents of office are tracked.	A memo will be created regarding moving suggestions to ensure that all contents are delivered in future moves.	The memo will be created by February 28, 2010.	1. Memo will be shared with supervisors at joint Unit Head meeting scheduled March 4, 2010. 2. Agenda will document those in attendance. Supervisors will share with unit staff.
4. CMISB staff will be trained on DOH HIPAA Policy P03.01-Minimum Necessary	Staff will learn to "limit the use, disclosure or request of PHI to the minimum necessary amount needed to accomplish the intended task".	DDD HIPAA Privacy Coordinator will provide training at next joint Unit Head meeting scheduled March 4, 2010. Unit supervisors to share training with unit staff.	1. DDD HIPAA Policy Coordinator will provide meeting agenda and sign-in sheet reflecting attendance. 2. Unit Supervisors will submit agenda and sign-in sheet for each unit to HIPAA Policy Coordinator at the next joint Unit Head meeting.
5. The forms committee will review the PHI elements contained on current DDD forms.	Forms will be evaluated as to the necessity of the PHI elements on forms. The committee will recommend the removal of PHI elements not necessary. The committee will submit changes to select forms to appropriate staff person for revision.	The forms committee will complete the review of the existing forms by March 31, 2010. Select forms will be revised and shared with Unit Supervisors by April 31, 2010. Unit supervisors will train/share with unit staff and new forms will be implemented immediately.	1. All form revisions will be provided to HIPAA Privacy Coordinator by April 31, 2010. 2. Evidence of training of new forms will be provided to HIPAA Privacy Coordinator no later that one month following the release of the revised forms.