

HIPAA HITECH Breach Toolkit

Category:	HIPAA Privacy and Security	Effective Date:	
Supersedes:	N/A	Version Number:	1.0
Applies to Covered Components and Support Units:	Aging Services, Children's Services, County Attorney's Office, Fire Rescue, Head Start, Health and Social Services, HIPAA Office, Human Resources, and Information Technology Services	HIPAA Security Rule Ref.:	164.308(a)(1)(i)

Purpose and Scope

State why the toolkit has been developed

Changes to the Health Insurance Portability and Accountability Act (HIPAA) were recently enacted under the Health Information Technology for Economic and Clinical Health Act (HITECH). These changes go into effect February of 2010. These changes affect covered entities and business associates. One major change for covered entities and business associates is they must now disclose if and when they have a security breach involving PHI. This toolkit contains the procedures and forms to assist in the capture and report of security breach information as HITECH requires.

State what business objectives, requirements, policies, and/or standards are being supported by the procedure

Health Insurance Portability and Accountability Act (HIPAA), and the Health Information Technology for Economic and Clinical Health Act (HITECH). This toolkit contains:

- Breach Notification Procedure
- Breach Work Plan
- Breach Incident Report Form
- Breach Notification Letter Template

Breach Notification Procedure

The following steps should be taken by Hillsborough County employees, HIPAA Liaisons and the HIPAA Committee when they become aware of a potential breach of Protected Health Information (PHI). A breach of PHI is the acquisition, access, use or disclosure of PHI in electronic or hard copy format, which compromises the security or privacy of the PHI. These steps are in groups according the type of employee:

- All Employees that have Access to PHI
- HIPAA Liaisons
- HIPAA Privacy and Security Office Staff (HIPAA Compliance Office Staff) and HIPAA Committee

Steps for Employees that have Access to PHI

1. If you think that there has been unauthorized access or disclosure to PHI, notify your supervisor and/or your HIPAA Liaison as soon as possible.
2. When you notify your supervisor and/or your HIPAA Liaison of a potential PHI breach, please include as much of the following information as you can (see the Breach Incident Report Form):

HIPAA HITECH Breach Toolkit

Category:	HIPAA Privacy and Security	Effective Date:	
Supersedes:	N/A	Version Number:	1.0
Applies to Covered Components and Support Units:	Aging Services, Children's Services, County Attorney's Office, Fire Rescue, Head Start, Health and Social Services, HIPAA Office, Human Resources, and Information Technology Services	HIPAA Security Rule Ref.:	164.308(a)(1)(i)

Breach Notification Procedure

- Facts about the potential breach; some examples include:
 - stolen or lost laptop, backup tape, or portable storage device
 - email or fax sent to the wrong person
 - paper or electronic records thrown in the trash
- Data elements; some examples include:
 - names
 - addresses
 - protected health information
 - Social Security Numbers
- Number of people affected
- Whether the information was encrypted
- Who was involved in the potential breach including witnesses

3. If you are a supervisor that has been notified of a potential PHI breach, please contact your HIPAA Liaison as soon as possible and give them the information about the breach so that they can determine whether the incident is a breach or if it is not a breach.

Steps for HIPAA Liaisons

1. Investigate all incidents that are potential breaches. Determine if the incident is a breach by answering these questions:
 - a. Does the incident include use or disclosure of PHI that is not allowed under the HIPAA Privacy Rule?
 - b. Does the incident compromise the privacy or security of PHI by creating significant risk of harm?
 - c. Is the incident excluded from the definition of a breach? Incidents that are excluded include:
 - An unintentional use of PHI by a workforce member acting in good faith and within the scope of his or her authority, and the PHI is not further used or disclosed improperly;
 - An inadvertent disclosure of PHI by an authorized person to another authorized person, and the PHI is not further used or disclosed; or
 - A disclosure of PHI to an unauthorized person where there is a good faith belief that the unauthorized person would not reasonably have been able to retain the PHI.

HIPAA HITECH Breach Toolkit

Category:	HIPAA Privacy and Security	Effective Date:	
Supersedes:	N/A	Version Number:	1.0
Applies to Covered Components and Support Units:	Aging Services, Children’s Services, County Attorney’s Office, Fire Rescue, Head Start, Health and Social Services, HIPAA Office, Human Resources, and Information Technology Services	HIPAA Security Rule Ref.:	164.308(a)(1)(i)

Breach Notification Procedure

If the answer to Step 1 a and/or b is yes, and the incident is not excluded from the definition of a breach as listed in c, or you are not sure of the answers to the questions above, then report the incident to the County’s HIPAA Compliance Office Staff as soon as possible. Follow Steps 2 and 3 of this procedure for documenting the incident.

If the answer to Step 1 a and b is no or the answer to Step 1 c is yes; report the incident in the HIPAA Compliance Tracking application. The report should include why the incident is not a privacy or security breach.

2. Collect, verify and document as much of the following information as you can:

- Facts about the potential breach; some examples include:
 - stolen or lost laptop, backup tape, or portable storage device
 - email or fax sent to the wrong person
 - paper or electronic records thrown in the trash
- Data elements; some examples include:
 - names
 - addresses
 - protected health information
 - Social Security Numbers
- Number of people affected
- Whether the information was encrypted
- Who was involved in the potential breach including witnesses

3. Report the incident in the HIPAA Compliance Tracking application as a Security Incident. The report should include the information verified in Step 2 of this procedure.

Steps for the HIPAA Compliance Office Staff and HIPAA Committee

1. The HIPAA Compliance Office Staff, with support from the HIPAA Committee, HIPAA Consultant and County Attorney, will verify that the incident meets the criteria of a Breach according to HIPAA, ARRA, HITECH, US Department of Health and Human Services (HHS) Breach Notification Rule and/or State guidelines. The HIPAA Compliance Office Staff will update the information in the HIPAA Compliance Tracking application as necessary. The HIPAA Compliance Office Staff and HIPAA

HIPAA HITECH Breach Toolkit

Category:	HIPAA Privacy and Security	Effective Date:	
Supersedes:	N/A	Version Number:	1.0
Applies to Covered Components and Support Units:	Aging Services, Children's Services, County Attorney's Office, Fire Rescue, Head Start, Health and Social Services, HIPAA Office, Human Resources, and Information Technology Services	HIPAA Security Rule Ref.:	164.308(a)(1)(i)

Breach Notification Procedure

Consultant will create a work plan, with input from the HIPAA Committee on appropriate task assignments and due dates. The work plan should contain the following steps as appropriate (see the Breach Work Plan):

- Document the incident, if it needs any additional documentation. For example, if the incident meets the HHS criteria of unsecured protected health information, check the HHS web site to confirm and update the latest report requirements.
- Notify the Individuals whose protected health information was involved in the breach (see the Breach Notification Letter Template). Notification to the Individual should be made as soon as possible and no later than 60 days after the breach is discovered. The Notice to the Individuals should include:
 - Description of the breach
 - Type of protected health information involved
 - What the Individuals need to do to protect themselves
 - What the County is doing to investigate the situation and prevent future breaches
 - County contact information that the Individual should contact with any questions that they have
- If the contact information for ten or more individuals is outdated or insufficient, the County must provide substitute notice in one of the following forms:
 - Conspicuous posting on the home page of the County web site for a period of ninety days; or,
 - In major print or broadcast media, including in the areas where the affected individuals likely reside. This notice must include a toll-free phone number where individuals can call and learn whether they are affected by the breach. The phone number must be active for at least 90 days.
- Notify the Media if the breach affects more than 500 people.
- Notify the HHS Secretary by visiting the HHS web site and filling out and electronically submitting a breach report form. If 500 or more individuals are affected, this notification should be at the same time that the individuals are notified. If less than 500 individuals, the HHS notification can be included in an annual log of events reported to HHS not later than 60 days following the end of the calendar year.
- Consult with the County Attorney's Office to determine if any other Federal or State law requires action for breach of protected health information and add the required action steps to the work plan.

HIPAA HITECH Breach Toolkit

Category:	HIPAA Privacy and Security	Effective Date:	
Supersedes:	N/A	Version Number:	1.0
Applies to Covered Components and Support Units:	Aging Services, Children’s Services, County Attorney’s Office, Fire Rescue, Head Start, Health and Social Services, HIPAA Office, Human Resources, and Information Technology Services	HIPAA Security Rule Ref.:	164.308(a)(1)(i)

Breach Notification Procedure

- Reassess privacy and security compliance policies, procedures, and training materials to determine what changes are needed. For example,
 - If the incident involved lost or stolen backup data, consider changing the procedures for transport and/or storage
 - If the incident was the result of employee error, consider retraining employees
 - If the incident was the result of a business associate’s error, consider terminating the agreement or imposing more stringent safeguards under the agreement
- Update the privacy and security compliance policies, procedures, training material and Notice of Privacy Practices as appropriate.
- Prepare for possible HHS-OCR or state Attorney General investigation.

Breach Work Plan Template

The following table contains work plan steps to assist the HIPAA Compliance Office Staff (lead) and HIPAA Committee in developing a Breach Work Plan. The “Tasks” column should be modified to include the relevant requirements for the Breach that occurred. The “Assigned To” column has a suggested position title in parenthesis; replace this with the appropriate person’s name. If more than one County Agency’s information has been breached, the HIPAA Liaisons listed should be for all Agencies that were affected by the breach. The “Date Due” column has the time after the incident in parenthesis as a guide; replace this with the actual Date Due. Keep in mind the reporting requirements when updating the Date Due.

Tasks	Assigned To	Date Assigned	Date Due	Status
1. Document the incident:				
a. Verify that the HIPAA Compliance Tracking application is up to date and accurate.	(HIPAA Liaison for Agency)		(First week)	
b. Check the HHS web site to confirm and update the latest report requirements.	(HIPAA Compliance Office Staff)		(First week)	
c. List all other Federal or State requirements for the breach. Include required tasks in this work plan.	(County Attorney [lead] and HIPAA Liaison for the Agency)		(First week)	
d. Document the investigation of the breach including who performed the investigation and who verified that the investigation is complete.	(HIPAA Liaison [lead] and HIPAA Committee)		(First week)	

HIPAA HITECH Breach Toolkit

Category:	HIPAA Privacy and Security	Effective Date:	
Supersedes:	N/A	Version Number:	1.0
Applies to Covered Components and Support Units:	Aging Services, Children's Services, County Attorney's Office, Fire Rescue, Head Start, Health and Social Services, HIPAA Office, Human Resources, and Information Technology Services	HIPAA Security Rule Ref.:	164.308(a)(1)(i)

Breach Work Plan Template

2. Notify the Individuals whose protected health information was involved in the breach. (See Breach Notification Letter Template for an outline)	(HIPAA Compliance Office Staff [lead] and HIPAA Committee)		(First two weeks)	
3. Determine if the contact information for ten or more individuals is outdated or insufficient. If it is, prepare notice for Hillsborough County Website, the notice should include the same information that is in the Breach Notification Letter.	(HIPAA Liaison [lead] and HIPAA Compliance Office Staff)		(First three weeks)	
4. Notify the Media if the breach affects more than 500 people.	(HIPAA Liaison [lead] HIPAA Committee and Public Relations Representative)		(First 30 days)	
5. Notify the HHS Secretary: if 500 or more individuals are affected, this notification should be at the same time that the individuals are notified by visiting the HHS web site and filling out and electronically submitting a breach report form. If less than 500 individuals, the HHS notification can be included in an annual log of events reported to HHS not later than 60 days following the end of the calendar year.	(HIPAA Liaison [lead] and HIPAA Committee)		(if 500 or more individuals are affected, this is at the same time as the individuals' notification.)	
6. Determine if any other Federal or State law requires action for breach of protected health information and add the required action steps to the work plan.	(HIPAA Liaison [lead] and Agency Attorney)		(First 30 days)	
7. Reassess privacy and security compliance policies, procedures, and training materials to determine what changes are needed. (See the Breach Assessment form for guidance)	(HIPAA Liaison [lead] and HIPAA Committee)		(First 45 days)	
8. Update the privacy and security compliance policies, procedures, training material and Notice of Privacy Practices as appropriate.	(HIPAA Liaisons for their agency's policy and procedure manual)		(First 60 days)	
9. Prepare for possible HHS-OCR or state Attorney General investigation.	(HIPAA Compliance Office [lead] and HIPAA Committee)		(First 60 days)	

Additional columns and rows may be added as needed for tasks and tracking the Breach Work Plan progress.

HIPAA HITECH Breach Toolkit

Category:	HIPAA Privacy and Security	Effective Date:	
Supersedes:	N/A	Version Number:	1.0
Applies to Covered Components and Support Units:	Aging Services, Children's Services, County Attorney's Office, Fire Rescue, Head Start, Health and Social Services, HIPAA Office, Human Resources, and Information Technology Services	HIPAA Security Rule Ref.:	164.308(a)(1)(i)

Breach Incident Report Form

Please complete this form and provide a copy to the HIPAA Compliance Office or your HIPAA Liaison.

Names of People Involved: Complete the following table with the names and contact information of the people involved in the Breach Incident (incident); names of the individuals whose information was included in the incident should be documented separately, so it can be maintained securely. Examples of roles that should be included in the table below are:

- Person(s) who Discovered the Incident
- Person(s) who Caused or Allowed the Incident
- Person(s) who Witnessed the Incident
- Agency(ies) whose Clients' information was involved in the Incident
- HIPAA Liaison(s) for the Agency(ies) whose Clients' information was involved in the Incident

Please add additional rows to the table if necessary.

Name (First Last)	Role	Phone Number	Email Address

Incident Date: _____ **Incident Time:** _____

Incident Location:

Incident Summary:

HIPAA HITECH Breach Toolkit

Category:	HIPAA Privacy and Security	Effective Date:	
Supersedes:	N/A	Version Number:	1.0
Applies to Covered Components and Support Units:	Aging Services, Children's Services, County Attorney's Office, Fire Rescue, Head Start, Health and Social Services, HIPAA Office, Human Resources, and Information Technology Services	HIPAA Security Rule Ref.:	164.308(a)(1)(i)

Incident Police Report Number (if applicable): _____

Other Information: _____

Breach Notification Letter Template

<Place Letter on Letter Head>

(Date)

M. _____(Name)

(Address)

(City, State Zip)

Dear M. _____(Name)

I am writing to notify you of a recent incident involving health information collected by Hillsborough County's _____
(Enter Department) Department. (Enter a summary of what happened including type of PHI involved)

(Enter what was done and is being done to mitigate harm, and to keep from happening again)

(Enter what steps the individual should take to protect themselves)

Hillsborough County's _____ (Enter Department or Division) Department / Division, as a health care provider, is required to comply with federal HIPAA privacy regulations and to follow established guidelines and policies to maintain the security of your health information, which it does. I want you to know that we take seriously our responsibility to ensure your privacy and have adopted extensive policies and educated our personnel to keep your health information secure and confidential. Nevertheless, occasionally mistakes occur which we do our best to correct and mitigate any potential further disclosure. Part of that process includes informing you of the occurrence and the steps taken.

HIPAA HITECH Breach Toolkit

Category:	HIPAA Privacy and Security	Effective Date:	
Supersedes:	N/A	Version Number:	1.0
Applies to Covered Components and Support Units:	Aging Services, Children's Services, County Attorney's Office, Fire Rescue, Head Start, Health and Social Services, HIPAA Office, Human Resources, and Information Technology Services	HIPAA Security Rule Ref.:	164.308(a)(1)(i)

I apologize for any inconvenience this disclosure may have caused and if you have any questions or would like any additional information, please contact me by calling (813) _____. In addition, you may also contact Hillsborough County's Privacy Officer, _____ at (813) _____ or by writing to him at P.O. Box 1110, Tampa, FL 33601-1110.

Sincerely,

 _____ (Enter Name)
 Hillsborough County _____ (Enter Department)
 _____ (Enter Address)
 Tampa, FL 33610-1433
 _____ (Enter Phone Number)
 _____ (Enter Email Address)

copy: _____, HIPAA Privacy & Security Officer

Revision History

Version	Rev. Date	Description of Change	Approved by
1.0	8/16/2010	Initial Draft	