

Georgia Department of Community Health

PRIVACY AND SECURITY POLICY AND PROCEDURE 436

INCIDENT RESPONSES

Effective Date: April 14, 2005

Updated: November 9, 2011

Approved: May 9, 2012



David A. Cook, Commissioner

**SCOPE:**

This policy and procedure applies to the entire DCH workforce, including permanent, temporary, full-time and part-time employees of DCH, employees of staffing companies who are on assignment with DCH, independent contractors who are working on an assignment for DCH, and volunteers who are providing services for DCH and are under the direct control of DCH.

**POLICY STATEMENT:**

It is the policy of the Department of Community Health (DCH) to respect the right of privacy of every individual and, in doing so, to safeguard the protected health information (PHI) of every individual whose information is maintained by DCH and by its contractors. DCH policy is to ensure compliance with all applicable laws that regulate the safeguarding of PHI, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH), and to establish and maintain a standard of best practices in safeguarding protected health information. The entire DCH workforce will actively participate in safeguarding PHI in any medium, including paper, electronic, and oral. Every workforce member must receive training before receiving access to DCH PHI. Failure to properly safeguard PHI will result in sanctions, up to and including termination of the existing relationship with DCH.

In the event that any member of the DCH workforce becomes aware of an incident he or she believes could result or has resulted in the unauthorized access, use, alteration, destruction, loss, or disclosure of PHI, the workforce member will immediately (upon becoming aware of the incident during the same business day) report the incident to the HIPAA Privacy and Security Officer in the Office of General Counsel, as provided in the Incident Response procedure. All incidents reported will be investigated as determined by and under the direction of the HIPAA Privacy and Security Officer with the assistance of the Incident Response Team and other staff as required.

**DEFINITIONS:**

**For purposes of this Incident Response Policy and Procedure, the following terms shall mean:**

**“Business Associate”** means an entity that creates or receives Protected Health Information in order to provide services to or on behalf of the DCH.

**“Breach”** means the acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI. For purpose of this definition, “compromises the security or privacy of the PHI” means poses a significant risk of financial, reputational, or other harm to the individual. A use or disclosure of PHI that does not include the identifiers listed at §164.514(e)(2), limited data set, date of birth, and zip code does not compromise the security or privacy of the PHI.

**“Access”** means the ability or means necessary to read, write, modify, or communicate data/information or otherwise use any protected health information.

**“DCH”** means the Georgia Department of Community Health.

**“Disclosure”** means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

**“HIPAA”** means the Health Insurance Portability and Accountability Act of 1996, enacted as Public Law 104-191, and implementing regulations.

**“HITECH Act”** means Title XIII of the American Recovery and Reinvestment Act of 2009 (the Health Information Technology for Economic and Clinical Health Act, or “HITECH”), and implementing regulations.

**“Incident”** means an event that a person reasonably believes to be an unauthorized use or disclosure of Individually Identifiable Health Information or a threat to the safety, availability, or accuracy of the Individually Identifiable Health Information.

**“Individually Identifiable Health Information”** means information, including demographic information from an individual, that:

- (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
- (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
  - (i) That identifies the individual; or
  - (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Any information that identifies an individual enrolled in a DCH managed health plan, or indicates that the individual is eligible for a DCH managed health plan, or shows that the individual received or will receive treatment or payment for treatment for any kind of medical condition, should be considered “individually identifiable health information” for purposes of this Policy and Procedure.

**“Law Enforcement Agency”** means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to investigate or

conduct an official inquiry into a potential violation of law; or prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

**“Privacy Rule”** means the rules and regulations promulgated pursuant to HIPAA and HITECH and codified in the Code of Federal Regulations at 45 C.F.R. §164.500, et sequitur.

**“Protected Health Information”** or **“PHI”** means individually identifiable health information that is transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium.

**“Security Rule”** means the rules and regulations promulgated pursuant to HIPAA and HITECH as codified in the Code of Federal Regulations at C.F.R. §164.302, et sequitur.

**“Unsecured Protected Health Information”** means Protected Health Information that is not encrypted or destroyed (shredded, if paper, or destroyed in a manner approved by the DCH IT department, if electronic). Unsecured Protected Health Information can include any information in any form of medium, including electronic, paper, or oral form.

**“Use”** means with respect to PHI, the sharing, employment, application, utilization, examination, or analysis of such information.

**“Workforce”** means permanent, temporary, full-time and part-time employees of DCH, employees of staffing companies who are on assignment with DCH, independent contractors who are working on assignment for DCH, and volunteers who are providing services for DCH and are under the direct control of DCH.

#### **INCIDENT RESPONSE TEAM RESPONSIBILITIES:**

The members of the Incident Response Team are the Chief Information Officer, the Information Security Officer, General Counsel, the Chief Operating Officer, the Director of Communications, the DCH Inspector General, the Remediation Specialist, and the HIPAA Privacy and Security Officer, or their designees. Ad hoc assistance to the Incident Response Team will be requested by the HIPAA Privacy and Security Officer based upon the incident and the assistance needed in order to fully investigate the incident and to perform any other activities related to the incident. It will be the responsibility of the DCH leadership team or designee to ensure that the required ad hoc assistance is available as needed.

##### **A. Commissioner**

- Work with the HIPAA Privacy and Security Officer and Director of Communications as necessary in order to convey the importance of safeguarding PHI and reporting incidents.
- Make reports of ongoing investigations to members of the Governor’s Executive Staff and the Board of Community Health, as appropriate.
- Work with the HIPAA Privacy and Security Officer and Director of Communications to review and approve all breach notifications within a timeframe that ensures compliance with breach notification deadlines.
- Work with the Chief Operating Officer, HIPAA Privacy and Security Officer, and Director of Communications to review and approve all changes to policies and

procedures or implement other remediation measures that require Commissioner approval.

#### **B. HIPAA Privacy and Security Officer**

- Review the initial report of the incident and determine whether to engage the Incident Response Team.
- In consultation with the Incident Response Team, take steps to mitigate harm.
- Ensure that the incident response procedure is implemented promptly and notify the Incident Response Team and Commissioner of any delays in implementing the incident response procedure.
- Oversee the investigation of the incident.
- In consultation with the General Counsel and the Incident Response Team, as applicable, review incidents to make a preliminary determination of whether a breach has occurred.
- Implement the Breach Notification Procedure, if a breach has occurred.
- Ensure the maintenance of documentation of incidents, investigations, reports, and other related data for a period of six (6) years, in accordance with applicable requirements of HIPAA.
- In collaboration with the Incident Response Team, ensure that the remediation plan is implemented or notify the Team and Commissioner that remediation has not been implemented.
- In collaboration with the Incident Response Team, ensure that appropriate sanctions are implemented or notify the Team and Commissioner that sanctions have not been implemented.
- Provide a final report of any breach to the General Counsel for the Commissioner, to include all relevant details of the investigation, a root cause analysis, an accounting of the disclosures, mitigation of harm, sanctions, and documentation.

#### **C. DCH Inspector General**

- Act as a liaison with law enforcement agencies upon reasonable belief that criminal activity has occurred.
- Obtain written documentation from the law enforcement agency of the reasons why any delay in notification is requested for purposes of the investigation.
- Coordinate with HIPAA Privacy and Security Officer, General Counsel, and law enforcement agency as needed in order for General Counsel to determine whether a delay in notification is permissible as a result of ongoing criminal investigation.

- Upon request of the HIPAA Privacy and Security Officer for assistance with the investigation, provide related direction and guidance to OIG staff necessary to support investigation.
- Ensure that remediation recommendations of the Remediation Specialist are documented, considered by the Incident Response Team and either approved or rejected.
- Provide documentation of all actions of OIG staff involved in an investigation to the HIPAA Privacy and Security Officer, in accordance with requirements of the HIPAA Privacy Rule for retention of records related to incidents for a period of six years.

**D. Chief Information Officer and Information Security Officer**

- Provide forensic analysis and any other assistance during the investigation.
- Identify “who, what, when, why, and how” of any incidents involving the impermissible use or disclosure of electronic PHI.
- Identify any needs for access level changes or terminations.
- Coordinate with Business Associates as needed to review audit logs and oversee any forensic investigation.
- Follow IT specific incident procedures.
- Provide a written report to the HIPAA Privacy and Security Officer regarding the relevant uses, disclosures, or access to electronic PHI.
- Provide system related documentation as needed to support the investigation.
- Authorize necessary and appropriate actions by Information Technology staff to support the incident investigation, mitigation, and remediation.
- Ensure the restoration of information systems resources and functionality as soon as practicable where operation of the systems may have been interrupted.
- Coordinate interaction with Georgia Technology Authority (GTA) as needed.
- Provide documentation of actions related to the incident response to the HIPAA Privacy and Security Officer for retention in accordance with the records retention requirements of the Privacy Rule and the Security Rule.

**E. General Counsel**

- Keep the Commissioner apprised as needed.
- Review reports prepared by the HIPAA Privacy and Security Officer.

- Identify contractual obligations of Business Associates and coordinate with vendor management to ensure that such obligations are satisfied during the investigation process.
- Assign responsibilities in the event that the HIPAA Privacy and Security Officer is unable to complete any or all of the responsibilities.
- Confer and coordinate with the Attorney General's Office as needed.
- Provide technical legal information and assistance.
- Coordinate with the Remediation Specialist, Chief Operating Officer, and HIPAA Privacy and Security Officer to ensure that contracts are amended as needed, and that contractual obligations related to the investigation, notification, and remediation are satisfied.

#### **F. Director of Communications**

- Ensure that all messaging is accurate, consistent, and properly vetted through the HIPAA Privacy and Security Officer and other members of the Incident Response Team as applicable.
- Prepare a press release, and talking points, as necessary, to address news media and legislative inquiries.
- Develop frequently asked questions (FAQs) that will anticipate and answer questions.
- Prepare staff for news media inquiries and interviews, as needed.
- Develop talking points to brief internal and external staff as needed.
- Provide guidance to the HIPAA Privacy and Security Officer and relevant management team as to the best method for providing substitute notice when more than ten individuals cannot be located.
- Coordinate with Business Associates' communications staff to ensure consistency of message.
- Submit media notification to the Commissioner for approval and publish notification after approval.
- After approval of notification by Commissioner, notify Governor's Office press/public relations office.

#### **G. Chief Operating Officer**

- Ensure that Vendor Management, Human Resources, and administrative support staff are deployed as needed for investigation and remediation.

- Ensure that pertinent administrative safeguards are reviewed, reinforced, and remediated as recommended in the interim and final reports of the incident investigated.
- Through Vendor Management, ensure that evidence of remediation by vendors is submitted to the Remediation Specialist.
- Provide documentation of actions related to the incident response to the HIPAA Privacy and Security Officer for retention in accordance with the records retention requirements of the HIPAA Privacy Rule and the HIPAA Security Rule.
- Ensure that appropriate sanctions for violations by contractors or employees are implemented, in accordance with recommendations of the HIPAA Privacy and Security Officer or, if applicable, the Incident Response Team.
- Ensure that all employees understand, as part of their performance management plan and the terms and conditions of employment, the requirement to report incidents as described in this policy and procedure.

#### **H. Remediation Specialist**

- Review reports of investigations and proposed corrective actions.
- Provide a written recommendation of remediation measures.
- Present the recommendation to the Incident Response Team.
- Review evidence that approved remediation plan has been implemented and report to Incident Response Team.

#### **I. Incident Response Team**

- Participate upon request or upon its initiative in the investigation of any privacy or security incident, as led by the HIPAA Privacy and Security Officer.
- Immediately determine the most appropriate and effective staff to serve as subject matter authority or authorities to address news media inquiries, as managed by the Communications staff and approved by the Commissioner.
- At the request of the Director of Communications or his or her staff designee, assist in the development of public information.
- Review the investigation findings and the report of the Remediation Specialist and approve a remediation action plan.
- Provide periodic updates daily as needed to the Commissioner's Office regarding status of investigation.
- Provide all records and other information to the HIPAA Privacy and Security Officer for the final report of the incident and maintenance of documentation.

## **REPORTING INCIDENTS:**

- Each member of the DCH workforce is responsible for immediately reporting all privacy and security incidents. "Immediately" means at least within the same day as the employee becomes aware of the incident.
- Initial reports of incidents should be made by email to [hipaa@dch.ga.gov](mailto:hipaa@dch.ga.gov), or by telephone to the HIPAA Privacy and Security Officer in the Office of General Counsel, or the Office of Inspector General, and shall include the name and contact information of the person reporting the incident, the names of all known parties or entities involved, and a description of any actions the reporting workforce member or others have taken in response.
- All initial reports of incidents received by the Office of General Counsel or Office of Inspector General shall be emailed to [hipaa@dch.ga.gov](mailto:hipaa@dch.ga.gov) or recorded in the applicable incident tracking system.
- An incident report form must be completed as soon as possible and submitted to the HIPAA Privacy and Security Officer. Forms are posted on the intranet, and the current form is attached to this procedure as Exhibit A.
- All incident report forms must be emailed to [hipaa@dch.ga.gov](mailto:hipaa@dch.ga.gov) and the email for the Inspector General.
- All incident report forms must be securely saved in a folder on the restricted O: HIPAA Privacy and Security Folder or in the approved incident tracking system.
- All members of the HIPAA Incident Response Team will have access to the restricted folder for HIPAA Privacy and Security.

## **INVESTIGATING INCIDENTS:**

- The HIPAA Privacy and Security Officer will lead all investigations.
- The HIPAA Privacy and Security Officer or his or her designee will work with the Incident Response Team during the investigation if necessary.
- The HIPAA Privacy and Security Officer or his or her designee will consult with General Counsel, the DCH Inspector General, or the Chief Information Officer within five days of receipt of notice of the incident and they will make written determination of whether the incident constituted an impermissible use or disclosure of Unsecured PHI under HIPAA or HITECH.
- If the incident was not an impermissible use or disclosure of Unsecured PHI, the HIPAA Privacy and Security Officer or his or her designee will notify the individual who reported the incident and document the decision in the incident file that was created.

- **If the incident WAS an impermissible use or disclosure of Unsecured PHI, the HIPAA Privacy and Security Officer will:**
  - Notify the Incident Response Team.
  - Coordinate further investigation with members of the Incident Response Team, as described in the “Incident Response Team” Section above.
  - Notify the Division Chief of the program impacted.
  - Notify Vendor Management and the relevant business owner, if the incident involves a Business Associate.
  - Identify any individuals harmed by the impermissible use or disclosure of Unsecured PHI.
  - Take immediate steps to mitigate any impermissible uses or disclosures, in coordination with the Information Security Officer if the incident involves electronic PHI.
  - If an impermissible disclosure occurred, make an entry in the PHI disclosure log that will enable DCH to produce an accounting of disclosures for an individual who requests one.
  - Meet with at least two of the following: General Counsel, Inspector General, and the Chief Information Officer to conduct a risk assessment using the Risk Assessment Checklist attached as Exhibit B to determine whether the impermissible use or disclosure compromised the security or privacy of PHI for purposes of the breach notification rules of HITECH. One step may include telephonic notice to one or more individuals if necessary in order to prevent imminent misuse or loss of Unsecured PHI. This notice does not substitute for the written notice described below. Obtaining a written statement that information improperly accessed was not used and was securely destroyed may support a finding that inadvertent access did not cause a risk of harm.
    - **If the impermissible use or disclosure DID NOT create a significant risk of harm**, the HIPAA Privacy and Security Officer or designee will prepare a written analysis of the information considered and the basis for the conclusion, notify the HIPAA Incident Response Team of the conclusion, and save the written analysis in applicable file on the restricted “HIPAA Privacy and Security” folder on the O Drive or in the incident tracking system.
    - **If the impermissible use or disclosure DID create a “significant risk” of harm**, then the “Breach Notifications” section below applies.

**BREACH NOTIFICATIONS:**

- If an impermissible use or disclosure of Unsecured PHI created a significant risk of harm, the HIPAA Privacy and Security Officer will implement the Breach Notification Procedure attached as Exhibit C.
- All notifications other than those required immediately in order to mitigate harm are subject to approval by the Commissioner or the Commissioner's designee.
- If the root cause analysis shows that one of DCH's Business Associates is responsible for the incident that resulted in the breach, in whole or in part, the HIPAA Privacy and Security Officer will notify General Counsel and vendor management to ensure that the Business Associate will provide all notices, will absorb all attendant costs, and will immediately indemnify DCH to the extent provided in the Business Associate contract.
- Content of all notifications is subject to approval by the HIPAA Privacy and Security Officer and the Commissioner, or Commissioner's designee, in the event notification is provided directly by a DCH Business Associate on behalf of the DCH.

**MITIGATION OF HARM:**

- The HIPAA Privacy and Security Officer or his or her designee will mitigate, to the extent practicable, any known harmful effect of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of the Privacy Rule or Security Rule by DCH or its contractors.
- Costs of mitigation will be paid by the entity responsible for causing the incident, as determined by the investigation.
- Mitigation may include the offer of credit monitoring or credit restoration for an affected individual or such other steps as reasonably may serve to reduce or prevent harm to the individual as a result of the incident.

**REMEDIATION:**

- Upon request of the HIPAA Privacy and Security Officer, the Remediation Specialist will review the final report of the incident and the documentation of the investigation and will prepare a report of recommended remediation measures.
- The Remediation Specialist will present the report to the Incident Response Team and Team members will fulfill their responsibilities to approve the remediation plan and support the implementation of the plan.
- Costs of the implementation of corrective actions will be paid by the entity responsible for causing the incident, as determined by the investigation.
- Remediation may include revisions to or development of policies and procedures, retraining, system modifications, revisions to practices and protocols, changes in supervision, imposition of sanctions or a combination of remedies and such other measures as may be necessary and appropriate to the incident.

- The Chief Operations Officer will provide evidence of remediation to the Remediation Specialist for review.
- The Remediation Specialist will review evidence of remediation and include reviews of similar evidence in accordance with auditing procedures in the future.
- Where remediation is found to be insufficient, additional actions will be implemented until the root cause of the incident has been corrected.

**DOCUMENTATION:**

- All documentation related to incident investigations will be compiled and maintained for a period of six (6) years, in accordance with the Privacy rule and Security Rule.
- The HIPAA Privacy and Security Officer will be responsible for the records retention under this policy and procedure.
- Access to records of incident investigations and reports will be available in accordance with the terms of applicable state and federal law and regulations.
- In no event will any protected health information of any individual be accessible as public record.
- All protected health information in documentation related to incidents will be protected by administrative, technical, and physical safeguards.

## Exhibit A

### PRIVACY/SECURITY INCIDENT REPORT FORM

**Report potential impermissible uses or disclosures of Protected Health Information by completing this form. The report should be emailed to [hipaa@dch.ga.gov](mailto:hipaa@dch.ga.gov) and Alison Earles, the DCH Privacy and Security Officer at [aearles@dch.ga.gov](mailto:aearles@dch.ga.gov), with a copy to Roy Griffis at [rgriffis@dch.ga.gov](mailto:rgriffis@dch.ga.gov) as soon as possible. Please write legibly.**

As required by the HIPAA Privacy and Security Policies and Procedures, I hereby submit the following information regarding a suspected impermissible use or disclosure of Protected Health Information.

Report Date: \_\_\_\_\_ Incident Date: \_\_\_\_\_

Person documenting incident:

Title	Phone	Work Unit / Section
-------	-------	---------------------

Person reporting incident: \_\_\_\_\_

Title	Phone	Work Unit / Section
-------	-------	---------------------

Date of discovery and Name of person who discovered	
Program(s) affected or involved	
Member(s) affected (Total number of Individuals and Names and contact information, as soon as available. Use separate pages as needed.)	
Technology system(s) affected or involved, if any	
Description of the incident as known to date (to be completed and confirmed through investigation)	

<p>Note whether a contractor, vendor or Business Associate was involved. If so, briefly describe actions and provide name(s) and how to contact for more information.</p>	
<p>Does this incident appear to be intentional or inadvertent (or unknown)?</p>	
<p>Description of follow-up action(s) taken to mitigate harm to individuals.</p>	
<p>Description of action(s) taken to reduce the possibility of recurrence.</p>	

Attach other pages or add information, as needed.

Exhibit B

DRAFT

Version 5/FINAL: 9/10/09

Revised 10/1/09; 10/15/09; 6/23/10; 8/19/10; 1/3/11 (Minor Revisions/Examples Attachment)  
Based on ARRA/HITTECH Interim Rules – August 24, 2009

Risk Assessment Analysis Tool

Note: For an acquisition, access, use or disclosure of PHI to constitute a breach, it must constitute a violation of the Privacy Rule

Q#	Question	Unsecured PHI	
		Yes - Next Steps	No - Next Steps
1	Was the impermissible use/disclosure unsecured PHI (e.g. not rendered unusable, unreadable, indecipherable to unauthorized individuals through the use of technology or methodology specified by the Secretary)?	Continue to next question	Notifications not required. Document decision.
<b>Minimum Necessary</b>			
2	Was more than the minimum necessary for the purpose accessed, used or disclosed?	Continue to next question	May determine low risk and not provide notifications. Document decision.
<b>Was there a significant risk of harm to the individual as a result of the impermissible use or disclosure?</b>			
3	Was it received and/or used by another entity governed by the HIPAA Privacy & Security Rules or a Federal Agency obligated to comply with the Privacy Act of 1974 & FISIA of 2002?	May determine low risk and not provide notifications. Document decision.	Continue to next question
4	Were immediate steps taken to mitigate an impermissible use/disclosure (ex. Obtain the recipients' assurances the information will not be further used/disclosed or will be destroyed)?	May determine low risk and not provide notifications. Document decision.	Continue to next question
5	Was the PHI returned prior to being accessed for an improper purpose (e.g. A laptop is lost/stolen, then recovered & forensic analysis shows the PHI was not accessed, altered, transferred or otherwise compromised)?	May determine low risk and not provide notifications. Document decision. Note: don't delay notification based on a hope it will be recovered.	Continue to next question
<b>What type and amount of PHI was involved in the impermissible use or disclosure?</b>			
6	Does it pose a significant risk of financial, reputational, or other harm?	Higher risk - should report	May determine low risk and not provide notifications. Document decision.

7	Did the improper use/disclosure only include the name and the fact services were received?	May determine low risk and not provide notifications. Document decision.	Continue to next question
8	Did the improper use/disclosure include the name and type of services received, services were from a specialized facility (such as a substance abuse facility), or the information increases the risk of ID Theft (such as SS#, account#, mother's maiden name)?	High risk - should provide notifications	Continue to next question
9	Was a limited data set [164.514(e)] or de-identified data [164.514(b)] used or disclosed? Note: take into consideration the risk of re-identification [164.514(c)] (the higher the risk, the more likely notifications should be made). <sup>21</sup>	Continued to next question	Continue to #11
10	Is the risk of re-identification so small that the improper use/disclosure poses no significant harm to any individuals (ex. Limited data set included zip codes that based on population features doesn't create a significant risk an individual can be identified)? <sup>22</sup>	May determine low risk and not provide notifications. Document decision.	Continue to next question
<b>Specific Breach Definition Exclusions</b>			
11	Was it an unintentional acquisition, access, or use by a workforce member acting under the organization's authority, made in good faith, within his/her scope of authority (workforce member was acting on the organization's behalf at the time), and didn't result in further use/disclosure (ex. billing employee receives an e-mail containing PHI about a patient mistakenly sent by a nurse (co-worker). The billing employee alerts the nurse of the misdirected e-mail & deletes it)?	May determine low risk and not provide notifications. Document decision.	Continue to next question
12	Was access unrelated to the workforce member's duties (ex. did a receptionist look through a patient's records to learn of their treatment)?	High risk - should provide notifications	Continue to next question
13	Was it an inadvertent disclosure by a person authorized to access PHI at a CE or BA to another person authorized to access PHI at the same organization, or its OHCA, and the information was not further used or disclosed (ex. A workforce member who has the authority to use/disclose PHI in that organization/OHCA discloses PHI to another individual in that same organization/OHCA and the PHI is not further used/disclosed)?	May determine low risk and not provide notifications. Document decision.	Continue to next question

<sup>21</sup> Updated 8/19/10.  
<sup>22</sup> Updated 8/19/10.

14	Was a disclosure of PHI made, but there is a good faith belief that the unauthorized recipient would not have reasonably been able to retain it (Ex: EOBs were mistakenly sent to wrong individuals and were returned by the post office, unopened, as undeliverable)?	May determine low risk and not provide notifications. Document decision.	Continue to next question. Note: if the EOBs were not returned as undeliverable, these should be treated as breaches.
15	Was a disclosure of PHI made, but there is a good faith belief that the unauthorized recipient would not have reasonably been able to retain it (ex. A nurse mistakenly hands a patient discharge papers belonging to a different patient, but quickly realized the mistake and recovers the PHI from the patient, and the nurse reasonable concludes the patient could not have read or otherwise retained the information)?	May determine low risk and not provide notifications. Document decision.	Document findings.

**Burden of Proof:** Required to document whether the impermissible use or disclosure compromises the security or privacy of the PHI (significant risk of financial, reputational, or other harm to the individual).

## Exhibit C

### Georgia Department of Community Health

#### HIPAA Protected Health Information Breach Notification Procedure

**Purpose:** Breach notification will be carried out in compliance with the American Recovery and Reinvestment Act (ARRA)/Health Information Technology for Economic and Clinical Health Act (HITECH) as well as any other federal or state notification law.

**Background:**

The American Recovery and Reinvestment Act of 2009 (ARRA) was signed into law on February 17, 2009. Title XIII of ARRA is the Health Information Technology for Economic and Clinical Health Act (HITECH). HITECH significantly impacts the Health Insurance Portability and Accountability (HIPAA) Privacy and Security Rules. While HIPAA did not require notification when patient protected health information (PHI) was inappropriately disclosed, covered entities may have chosen to include notification as part of the mitigation process. HITECH does require notification of certain breaches of unsecured PHI to the following: individuals, Department of Health and Human Services (HHS), and the media. The effective implementation for this provision is September 23, 2009 (pending publication HHS regulations).

**Definitions:**

**Access:** Means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.<sup>1</sup>

**Breach:** Means the acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI. For purpose of this definition, "compromises the security or privacy of the PHI" means poses a significant risk of financial, reputational, or other harm to the individual. A use or disclosure of PHI that does not include the identifiers listed at §164.514(e)(2), limited data set, date of birth, and zip code does not compromise the security or privacy of the PHI.

Breach excludes:

1. Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of a Covered Entity (CE) or Business Associate (BA) if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule.
2. Any inadvertent disclosure by a person who is authorized to access PHI at a CE or BA to another person authorized to access PHI at the same CE or BA, or organized health care arrangement in which the CE participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule.
3. A disclosure of PHI where DCH has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such

---

<sup>1</sup>45 CFR § 164.304.

information.<sup>2</sup>

Covered Entity: A health plan, health care clearinghouse, or a healthcare provider who transmits any health information in electronic form.<sup>3</sup>

Disclosure: Disclosure means the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.<sup>4</sup>

Individually Identifiable Health Information: That information that is a subset of health information, including demographic information collected from an individual, and is created or received by a health care provider, health plan, employer, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.<sup>5</sup>

Law Enforcement Official: Any officer or employee of an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to investigate or conduct an official inquiry into a potential violation of law; or prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.<sup>6</sup>

Organization: For the purposes of this policy, the term "organization" shall mean the covered entity to which the policy and breach notification apply.

Protected Health Information (PHI): Protected health information means individually identifiable health information that is: transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium.<sup>7</sup>

Unsecured Protected Health Information: Protected health information (PHI) that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Pub. L. 111-5 on the HHS website.

1. Electronic PHI has been encrypted as specified in the HIPAA Security rule by the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key and such confidential process or key that might enable decryption has not been breached. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt.<sup>8</sup> The following encryption processes meet this standard.

<sup>2</sup> ARRA/HITECH Title XIII Section 13400; §164.402,

<sup>3</sup> 45 CFR § 160.103.

<sup>4</sup> 45 CFR § 160.103.

<sup>5</sup> 45 CFR § 164.503.

<sup>6</sup> 45 CFR § 164.103.

<sup>7</sup> 45 CFR § 164.503.

<sup>8</sup> 45 CFR Parts 160 and 164; Final Rules Issued 8/19/09.

- A. Valid encryption processes for data at rest (i.e. data that resides in databases, file systems and other structured storage systems) are consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.
  - B. Valid encryption processes for data in motion (i.e. data that is moving through a network, including wireless transmission) are those that comply, as appropriate, with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, and may include others which are Federal Information Processing Standards FIPS 140-2 validated.
2. The media on which the PHI is stored or recorded has been destroyed in the following ways:
- A. Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.
  - B. Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publications 800-88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved.<sup>9</sup>

**Workforce:** Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.<sup>10</sup>

**Policy Statement/s:**

1. **Discovery of Breach:** A breach of PHI shall be treated as “discovered” as of the first day on which such breach is known to DCH or its Business Associate, or, by exercising reasonable diligence would have been known. An organization is deemed to have knowledge of a breach if such breach is known or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent (business associate) of the organization.
2. **Risk Assessment:** For an acquisition, access, use or disclosure of PHI to constitute a breach, it must constitute a violation of the Privacy Rule. A use or disclosure of PHI that is incident to an otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper minimum necessary procedures would not be a violation of the Privacy Rule and would not qualify as a potential breach. To determine if an impermissible use or disclosure of PHI constitutes a breach and requires further notification to individuals, media, or the HHS secretary under breach notification requirements, DCH will need to perform a risk assessment to determine if there is significant risk of harm to the individual as a result of the impermissible use or

<sup>9</sup> HHS issued guidance on protecting personally identifiable healthcare information; document was the work of a joint effort by HHS, its Office of the National Coordinator for Health Information Technology and Office for Civil Rights, and the CMS (Issued 4/17/09).

<sup>10</sup> 45 CFR § 164.103.

disclosure.<sup>11</sup> The organization shall document the risk assessment as part of the investigation in the incident report form noting the outcome of the risk assessment process. The organization has the burden of proof for demonstrating that all notifications were made as required or that the use or disclosure did not constitute a breach. Based on the outcome of the risk assessment, the organization will determine the need to move forward with breach notification. The risk assessment and the supporting documentation shall be fact specific and address:

- A. Consideration of who impermissibly used or to whom the information was impermissibly disclosed.
  - B. The type and amount of PHI involved.
  - C. The potential for significant risk of financial, reputational, or other harm.
3. Timeliness of Notification: Upon determination that breach notification is required, the notice shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach by the organization involved or the business associate involved. It is the responsibility of the organization to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of delay.
4. Delay of Notification Authorized for Law Enforcement Purposes: If a law enforcement official states to the organization that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, the organization shall:
- A. If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting of the timer period specified by the official; or
  - B. If the statement is made orally, document the statement, including the identify of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.<sup>12</sup>
5. Content of the Notice: The notice shall be written in plain language and must contain the following information:
- A. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
  - B. A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved).
  - C. Any steps the individual should take to protect themselves from potential harm resulting from the breach.
  - D. A brief description of what the organization is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.

---

<sup>11</sup> The organization may choose to make the decision to notify patients of a breach even after completion of the risk assessment indicates that there is no requirement to do so under ARRA/HITECH.

<sup>12</sup> 45 CFR § 164.412.

- E. Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, Web site, or postal address.

6. Methods of Notification: The method of notification will depend on the individuals/entities to be notified. The following methods must be utilized accordingly:

A. Notice to Individual(s): Notice shall be provided promptly and in the following form:

1. Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification shall be provided in one or more mailings as information is available. If the organization knows that the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first-class mail to the next of kin or person representative shall be carried out.
2. Substitute Notice: In the case where there is insufficient or out-of-date contact information (including a phone number, email address, etc.) that precludes direct written or electronic notification, a substitute form of notice reasonably calculated to reach the individual shall be provided. A substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative.
  - a. In a case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then the substitute notice may be provided by an alternative form of written notice, telephone, or other means.
  - b. In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then the substitute notice shall be in the form of either a conspicuous posting for a period of 90 days on the home page of the organization's website, or a conspicuous notice in a major print or broadcast media in the organization's geographic areas where the individuals affected by the breach likely reside. The notice shall include a toll-free number that remains active or at least 90 days where an individual can learn whether his or her PHI may be included in the breach.
3. If the organization determines that notification requires urgency because of possible imminent misuse of unsecured PHI, notification may be provided by telephone or other means, as appropriate in addition to the methods noted above.

B. Notice to Media: Notice shall be provided to prominent media outlets serving the state and regional area when the breach of unsecured PHI affects more than 500 patients. The Notice shall be provided in the form of a press release.

C. Notice to Secretary of HHS: Notice shall be provided to the Secretary of HHS as follows below. The Secretary shall make available to the public on the HHS

Internet website a list identifying covered entities involved in all breaches in which the unsecured PHI of more than 500 patients is accessed, acquired, used, or disclosed.<sup>13</sup>

1. For breaches involving 500 or more individuals, DCH shall notify the Secretary of HHS as instructed at [www.hhs.gov](http://www.hhs.gov) at the same time notice is made to the individuals.
  2. For breaches involving fewer than 500 individuals, DCH will maintain a log of the breaches and annually submit the log to the Secretary off HHS during the year involved (logged breaches occurring during the preceding calendar year to be submitted no later than 60 days after the end of the calendar year). Instructions for submitting the log are provided at [www.hhs.gov](http://www.hhs.gov).<sup>14</sup>
7. Maintenance of Breach Information/Log: As described above and in addition to the reports created for each incident, the HIPAA Privacy and Security Officer shall maintain a process to record or log all breaches of unsecured PHI regardless of the number of patients affected.<sup>15</sup> The following information should be collected/logged for each breach (see sample Breach Notification Log):
- A. A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of patients affected, if known.
  - B. A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, etc.).
  - C. A description of the action taken with regard to notification of patients regarding the breach.
  - D. Resolution steps taken to mitigate the breach and prevent future occurrences.
8. Business Associate Responsibilities: DCH Business Associates shall notify DCH of suspected impermissible uses or disclosures of PHI within the deadline set forth in the Business Associate Agreement. All Business Associates shall comply with the requirements of the Business Associate Agreement and cooperate with DCH in order to ensure that breach notifications are made in accordance with the law.

<sup>13</sup> Note: If the breach involves "secured" PHI, no notification needs to be made to HHS.

<sup>14</sup> For calendar year 2009, the organization is required to submit information to the HHS secretary for breaches occurring after the September 23, 2009 effective implementation date.

<sup>15</sup> The organization shall delegate this responsibility to one individual (e.g., Privacy Officer).