

# Georgia Department of Community Health

## PRIVACY AND SECURITY POLICY AND PROCEDURE

### INCIDENT RESPONSES

**Effective Date:** April 14, 2005

**Updated:** April 16, 2007

#### **SCOPE:**

This policy and procedure applies to the entire DCH workforce, including employees, volunteers, trainees, and other persons whose conduct, in the performance of work for DCH, is under the direct control of DCH, whether or not they are paid by DCH. The applicability of the policy to contractors and subcontractors whose duties on behalf of and for DCH involve the use or disclosure of protected health information shall be through the Business Associate Agreement that shall be signed by each entity or person, other than members of the DCH workforce, whose services for DCH involve the use or disclosure of protected health information.

#### **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 used or disclosed by DCH and by its contractors. DCH policy is to ensure compliance with all applicable laws, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and to establish and maintain a standard of best practices in safeguarding protected health information. The entire DCH workforce will actively participate in safeguarding protected health information in any medium, including paper, electronic and oral. DCH prioritizes all work efforts related to all facets protecting health information including reporting, notification, and investigation.

In the event that any member of the DCH workforce becomes aware of an incident resulting in the unauthorized access, use, alteration, destruction, loss, or disclosure of protected health information, the staff member will immediately (upon becoming aware of the incident during the same business day) report the incident to the Director of Compliance 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 Director of Compliance 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:

“Access” means the ability or the 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 (DCH or a contractor or subcontractor) holding the information.

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

“Incident” means the unauthorized: access, use, disclosure, loss, modification, destruction or interference with protected health information, whether attempted or successful.

“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.

“Privacy Rule” means the rules and regulations promulgated pursuant to HIPAA 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:

- (iii) Transmitted by electronic media;
- (iv) Maintained in electronic media; or
- (v) Transmitted or maintained in any other form or medium.

**“Security Rule”** means the rules and regulations promulgated pursuant to HIPAA and codified in the Code of Federal Regulations at 45 C.F.R. §164.302, et sequitur.

**“Use”** means, with respect to PHI, the sharing, employment, application, utilization, examination, or analysis of such information within an entity (DCH or a contractor or subcontractor) that maintains such information.

**“Workforce”** means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for DCH, is under the direct control of DCH, whether or not they are paid by DCH.

### **INCIDENT RESPONSE TEAM:**

The members of the Incident Response are the Chief Information Officer, the General Counsel, the Chief Operating Officer, the Chief of Communications, the DCH Inspector General, and the Director of Compliance, or the designee of any member. Ad hoc assistance to the Incident Response Team will be requested by the Director of Compliance 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.

### **RESPONSIBILITIES**

#### **A. Commissioner**

- Will make reports to members of Governor’s Executive Staff and the Board of Community Health, as appropriate.

#### **B. Director of Compliance**

- Serving as the DCH Privacy and Security Officer, review the initial report of the incident and determine whether to engage the Incident Response Team.
- Ensure that the incident response procedure is implemented promptly and appropriately, including investigation, an accounting of disclosures for each individual affected, mitigation, sanctions, remediation and documentation.
- Lead the investigation of the incident.
- In consultation with the General Counsel and the Incident Response Team, as applicable, review incidents to make preliminary determination of whether notification is appropriate, subject to approval by the Commissioner, and direct the notification process.
- Provide interim reports as needed to General Counsel.

- Prepare notices of incidents as needed for the Office for Civil Rights (OCR) and the Centers for Medicare and Medicaid Services (CMS) of the U.S. Department of Health and Human Services and the Attorney General of Georgia.
- 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 appropriate remediation is implemented.
- Provide a final report of the incident to the General Counsel for the Commissioner, to include all relevant details of the investigation, a root cause analysis, an accounting of disclosures, mitigation, sanctions and documentation.

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

- Act as a liaison with law enforcement agencies upon reasonable belief that criminal activity has occurred.
- Upon request of the Director of Compliance for assistance with the investigation, provide related direction and guidance to OIG staff necessary to support investigation.
- In collaboration with the Incident Response Team, through its Office of Audits ensure that appropriate remediation is implemented.
- Provide documentation of all actions to the Director of Compliance, 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**

- 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.
- Assist the Communications staff in development of accurate public information, with particular regard to technical safeguards and technology issues.
- Coordinate interaction with Georgia Technology Authority (GTA) as needed.
- Provide documentation of actions related to the incident response to the Director of Compliance for retention in accordance with the records retention requirements of the HIPAA Privacy Rule and the HIPAA Security Rule.

### **E. General Counsel**

- Keep the Commissioner apprised as needed.
- Monitor the participation by the Director of Compliance.

- Confer and coordinate with the Attorney General's Office as needed.
- Provide technical legal information and assistance.
- Notify Governor's Office General Counsel.

#### **F. Chief of Communications**

- Develop talking points to address news media and legislative inquiries and to ensure consistent messaging.
- Develop frequently asked questions (FAQs) that will anticipate questions.
- Prepare staff for news media inquiries and interviews, as needed.
- Develop talking points to brief internal and external staff as needed.
- Determine the need of public notice, advise Commissioner and publish notice upon request.
- 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.
- Ensure that pertinent administrative safeguards are reviewed, reinforced and remediated as recommended in the interim and final reports of the incident investigation.
- Provide documentation of actions related to the incident response to the Director of Compliance 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 Director of Compliance or, if applicable, the Incident Response Team.
- Ensure that all employees as a part of their performance management plan will have under terms and conditions of employment the requirement to report incidents as described in this policy and procedure.

#### **H. Incident Response Team**

- Participate upon request or upon its initiative in the investigation of any privacy or security incident, as led by the Director of Compliance.
- Immediately determine the most effective and appropriate staff to serve as subject matter authority or authorities to address news media inquiries, as managed by the Communications staff.
- As led by the Chief of Communications or her staff designee, assist in the development of public information.
- Review and confer about the investigation findings in order to identify effective mitigation and remediation.

- Provide periodic updates daily as needed to Commissioner's Office regarding status of investigation.
- Provide all records and other information to Director of Compliance for the final report of the incident and for maintenance of documentation.

## **I. Management Team**

- Review and analyze all final reports and corrective actions.
- Review policies and procedures and determine gaps.
- Implement and communicate policy changes to applicable staff.
- Review and discuss "lessons learned" and what has been done to mitigate risk of recurrence.
- Provide documentation of all actions to the Director of Compliance, in accordance with requirements of the HIPAA Privacy Rule for retention of records related to incidents for a period of six years.

## **PROCEDURE:**

### **A. Reporting**

- Each member of the DCH workforce is responsible for immediately reporting all privacy and security incidents. "Immediately" means at least within the same day the employee becomes aware of an incident.
- A form for reporting is located on the DCH intranet; however, use of the form is encouraged but is not mandatory. Promptness in reporting is of the utmost importance.
- Reports of incidents may be made by email, telephone, on paper (using the form or not) or in person.
- Reports must include all of the following data that is available to the reporting person at the time of the initial report:
  1. The reporting person's contact information,
  2. The names of all known parties involved in the incident (whether entities or individuals),
  3. A description of what happened,
  4. A general description of the information involved,
  5. Any related actions that an employee has taken or of which the employee is aware; and
  6. Any other related information.
- Reports will be transmitted to Director of Compliance and to all members of the Department's Management Team using priority messaging via secure group email. Any use or disclosure of PHI will only be included in email if the email is encrypted. No person will send or forward any message that contains PHI without encryption if electronic or without application of stringent safeguards for all other media of communication.

## **B. Investigation**

- The Director of Compliance, serving as the Privacy and Security Officer, will lead and direct the investigation.
  1. Review the initial report and determine the appropriate next steps.
  2. Ensure that all relevant details are obtained, including supporting documentation.
  3. Provide interim reports to the General Counsel.
  4. Make a preliminary analysis of the scope and impact of the incident.
  5. Based upon the preliminary analysis, request participation by the Incident Response Team as needed.
- The report of the investigation will include recommendations by the Director of Compliance or the Incident Response Team, as applicable, for notification, mitigation and remediation.
- The report of the investigation will become a part of the final incident report, which will be among the documentation maintained in accordance with the HIPAA Privacy Rule.

## **C. Notification**

- All notifications are subject to approval by the Commissioner or the Commissioner's designee.
- Notifications are necessarily incident-specific but generally will include the following:
  1. A general description of what happened;
  2. A general description of the information involved;
  3. Mitigation steps taken by DCH or the contractor responsible;
  4. Contact information for additional information or to obtain assistance;
  5. Where appropriate, information to prevent identify theft such as:
    - Instructions and materials to obtain a free credit report.
    - Instructions and materials to obtain a fraud alert.
- Notifications will be written in terminology that is readily understood by the majority of the individuals who are affected.
- If the root cause analysis shows that one of DCH's contractors is responsible for the incident, the contractor will provide all notices, will absorb all attendant costs and will indemnify DCH, as provided in the contract.
- Content of all notifications is subject to approval by DCH, in the event notification is provided directly by a DCH contractor.
- Notification to the Governor's office and the Board of Community Health will be made by the Commissioner or the Commissioner's designee.

#### **D. Mitigation**

- DCH 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 HIPAA 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 for an affected individual or such other steps as reasonably may serve to reduce or avoid harm to the individual as a result of the incident.

#### **E. Remediation**

- DCH will ensure that necessary and appropriate corrective actions are identified and implemented as soon as possible following an incident.
- 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.
- DCH will monitor the remediation subsequent to implementation and monitor periodically at random thereafter, in order to ensure that the corrective actions have been successful.
- Where remediation is found to be insufficient, additional actions will be implemented until the root cause of the incident has been corrected successfully.
- A data entry will be made into a disclosure log that will enable DCH to produce an accounting of disclosures for an individual upon request.

---

#### **F. Documentation**

- All documentation related to incident investigations will be compiled and maintained for a period of six (6) years, in accordance with the HIPAA Privacy Rule and Security Rule.
- The Director of Compliance 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 data element of 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.

## External Notifications

The following public entities will be notified of incidents involving DCH health plans:

	Medicaid	SHBP	Other
<b>Federal</b>			
HHS' Office for Civil Rights (OCR) (HIPAA Privacy Rule enforcement)	X	X	X
HHS' Centers for Medicare and Medicaid Services (CMS) (HIPAA Security Rule enforcement)	X	--	--
<b>State</b>			
Governor's Office	X	X	X
Board of Community Health	X	X	X
Georgia Technology Authority (GTA)	If applicable	If applicable	If applicable
Georgia Merit System (GMS)	--	If applicable	--
Attorney General's Office	X	X	X
Department of Administrative Services (DOAS) Risk Management Division	X	X	X
<b>News Media</b>			
All media through public notice	X	X	If applicable

## PRIVACY OR SECURITY INCIDENT REPORT FORM

**Report potential violations of the HIPAA Privacy Rule or the HIPAA Security Rule using this form. The report should be provided to Ruth Carr, Deputy General Counsel and the DCH Privacy and Security Officer, 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 possible violation of the HIPAA Privacy or Security Rule.

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 or Names, 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)	
Note whether a contractor, vendor	

<p>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.