

PRV - Reporting a Health Insurance Portability Accountability Act (HIPAA) Incident to the Contract Administration Office (CAO)

Purpose:

The purpose of this procedure is to identify, resolve and report a HIPAA violation to the State. As a contractor, Provider Services staff have in their possession necessary Protected Health Information (PHI) that is disclosed by the State to perform its obligations under the contract.

Identification of Roles:

Primary Role- Provider Services Associate Analyst

Performance Standards:

N/A

Path of Business Procedure:

Step 1: Receive concern or complaint

- a. The Customer Service Representative (CSR) receives a call or written correspondence from the provider stating that the provider received correspondence or documentations that did not belong to them.

Step 2: Complete HIPAA Compliance Incident Report

- a. The staff member completes the HIPAA Compliance Incident Report and attaches available OnBase documentation that relates to the incident and forwards the report via e-mail to the Associate Analyst at lhuber@dhs.state.ia.us

Step 3: E-mail the form to the Associate Analyst

- a. The Associate Analyst reviews the complaint and ensures that all documentation is attached and completes the form to report a breach of unsecured protected health information before forwarding it to the Contract Administration Office (CAO).

Step 4: Report the incident and resolution

- a. The Associate Analyst emails the incident report and documentation to the CAO, Stephanie Clark (Sclark2@dhs.state.ia.us) with a copy to the Department of Human Services (DHS) Unit Manager and Provider Services Account Manger

Step 5: Save the email

- a. The Associate Analyst saves the e-mail sent to the CAO in the folder titled HIPAA Incidents found in the Associate Analyst's personal share drive.

Forms/Reports:

Provider Services HIPAA Compliance Incident Report
Information Security Date Breach Incident Report DHS Information Security and Privacy Office

RFP References:

N/A

Interfaces:

CAO

Attachments:

Provider Services HIPAA Compliance Incident Report
Information Security Data Breach Incident Report DHS Information Security and Privacy Office
Process Map

PROVIDER SERVICES
HIPAA COMPLIANCE INCIDENT REPORT:

Please complete this form to report a security incident. All incidents are to be reported immediately. E-mail this form to Linda Huber. lhuber@dhs.state.ia.us

REPORTED BY:

DATE:

PROVIDER NAME:

PROVIDER NUMBER:

PROVIDER PHONE NUMBER:

DESCRIPTION OF INCIDENT: _____

DATE OF INCIDENT:

TIME OF INCIDENT:

WHAT WAS DONE TO CORRECT THE INCIDENT?



Iowa Department of Human Services
Information Security Data Breach Incident Report
DHS Information Security and Privacy Office

All security and privacy incidents must be reported to, and a copy of this form filed with a supervisor and the DHS Security and Privacy Office.

Stolen or lost laptops must be reported to DHS Information Security and Privacy Office immediately.

Today's Date [REDACTED]	Date and Time that Security Incident Happened Date [REDACTED] Time [REDACTED]
Date Security Incident was Discovered [REDACTED]	Date Security Incident First Reported [REDACTED]
DHS Division Involved in the Security Incident [REDACTED]	
If a DHS contractor was involved: Contractor Name [REDACTED]	Contract Number [REDACTED]



Incident Reporter	
Name [REDACTED]	Title [REDACTED]
Phone [REDACTED]	Mobile [REDACTED]
Email [REDACTED]	
Address [REDACTED]	

Computer or Data Owner/User	
Name [REDACTED]	Title [REDACTED]
Phone [REDACTED]	Email [REDACTED]
Address [REDACTED]	
Provide a description of the Incident: [REDACTED]	

Type of Incident Detected (check all that apply)		
<input type="checkbox"/> Virus/malicious code	<input type="checkbox"/> Unauthorized software	<input type="checkbox"/> Denial of service attack
<input type="checkbox"/> Unauthorized access	<input type="checkbox"/> User account compromised	<input type="checkbox"/> Unauthorized physical access
<input type="checkbox"/> Confidential data breach	<input type="checkbox"/> System stolen or lost	<input type="checkbox"/> Other: _____

Information on Affected Systems (if multiple, attach list)		
Type of computer or media:		
<input type="checkbox"/> Desktop	<input type="checkbox"/> Laptop/tablet	<input type="checkbox"/> Server
<input type="checkbox"/> Paper document	<input type="checkbox"/> Portable media (flashdrive, DVD, etc.)	
Was the data or system encrypted? <input type="checkbox"/> Yes <input type="checkbox"/> No		
Other information available: _____		

Incident Assessment		
Was this incident a threat to a critical agency/facility service?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Was this incident a threat to a client's confidentiality?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
How many individual records are involved? _____		
How many individual (patients) are impacted? _____		
If the number of individual (patients) impacted is over 500, does the security incident impact more than 500 individuals who live in the same state?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Are any of the individuals impacted minors?	<input type="checkbox"/> Yes	<input type="checkbox"/> No

Sensitivity of the Data Residing on System (Check for "Yes")		
<input type="checkbox"/>	Names of applicants or recipients of DHS services? (Iowa Code § 217.30)	
<input type="checkbox"/>	An individual's first name or first initial and last name? (Iowa Code ch. 715C)	
<input type="checkbox"/>	Information concerning the social or economic conditions or circumstances of particular individuals who are now receiving or have received services or assistance from DHS? (Iowa Code § 217.30)	
<input type="checkbox"/>	Information received for verifying income eligibility and amount of medical assistance payments regarding a particular individual? (42 CFR § 431.300)	
<input type="checkbox"/>	Drivers' license numbers or other unique identification number created or collected by a government body? (Iowa Code ch. 715C)	
<input type="checkbox"/>	State identification numbers?	
<input type="checkbox"/>	Any unique identification number created or collected by a governmental agency? (Iowa Code ch. 715C)	
<input type="checkbox"/>	Unique electronic identifier or routing code, in combination with any required security code, access code, or password that would permit access to an individual's financial account? (Iowa Code ch. 715C)	

- Any unique identification number created or collected by a governmental agency? (Iowa Code ch. 715C)
- Information about an identifiable individual's diagnosis or treatment for HIV or AIDS? (Iowa Code § 141A.9)
- Information about an identifiable individual's treatment for substance abuse? (42 CFR pt. 2)
- Addresses of applicants or recipients of DHS services? (Iowa Code § 217.30)
- Details of the types of services or amounts of assistance provided to identifiable individuals? (Iowa Code § 217.30)
- Agency evaluations of information about a particular identifiable individual? (Iowa Code § 217.30)
- Medical or psychiatric data, including diagnosis and past history of disease or disability, concerning a particular individual? (Iowa Code § 217.30)
- Social security numbers? (Iowa Code ch. 715C)
- Child abuse information, assessments, or reports?
- Financial account numbers, credit card numbers, or debit card numbers that were disclosed along with a security code or some form of password that would permit access to an individual's financial accounts? (Iowa Code ch. 715C)
- Unique biometric data, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data? (Iowa Code ch. 715C)
- Information created or received by a division of DHS covered by HIPAA regulations that relates to care provided or physical or mental status of an identifiable individual or with which you reasonably believe could be used to identify the individual? (HIPAA regulations)
- Information about an identifiable individual's mental health? (Iowa Code chs. 228, 229)
- Information received in connection with the identification of legally liable third party resources of an identifiable individual? (42 CFR §§ 431.300-431.307)

Notifications

- Was local law enforcement notified? Yes No
- Was supervisor notified? Yes No

Actions Taken To-Date

What actions have been taken to mitigate any damage from this breach or to protect against further breaches?

When completed, save all changes, attach, and email to: dcoving@dhs.state.ia.us

