

**HIV/AIDS Section (HAS)**  
**Protocol for Breaches of Confidentiality of CAREWare Data**

**A. Purpose**

This protocol outlines the steps that will be taken when there is a breach of protected health information entered into CAREWare. The protocol is intended to supplement DOHP 50-10-10 Information and Security Policy or local policies written to conform to the security requirements of Department of Health HIV/AIDS patient care contracts and subcontracts. More restrictive state or federal rules, regulations or laws take precedent over this protocol.

**B. Definitions**

1. *Breach of confidentiality of CAREWare data* - Occurs when individual identifiers, as described in "Confidential CAREWare Client Identifiers" (Appendix A), are accessed by or shared with person(s) who are not legally authorized to know a client's HIV status or other protected health information.
2. *Electronic breach of confidentiality of CAREWare data* - occurs when individual identifiers, as described in "Confidential CAREWare Client Identifiers" (Appendix A), are electronically transmitted unencrypted or accessed or shared with person(s) who are not legally authorized to know a client's HIV status or other protected health information.

**C. Procedure**

1. For a first offense of breach of confidentiality of CAREWare data:
  - a. HAS will notify the user of the breach and the user will be locked out of CAREWare until the steps in paragraphs 1.b-d are completed.
  - b. HAS will notify the user's supervisor and/or the executive administrator of the user's organization of the seriousness of this issue and require an acknowledgement by their supervisor/administrator in writing. An e-mail to the HAS staff making the notification is acceptable written acknowledgement.
  - c. HAS staff will report the breach to the section's Information Security and Privacy Coordinator, who will submit an Incident Report. Depending on the severity of the breach, the Incident Report will be sent to the Division of Disease Control and Health Protection's (division) security officer or the Department's Inspector General for review.
  - d. If an electronic breach of confidentiality of CAREWare data is by unencrypted transmission via e-mail, the sender and all recipients will be instructed to double- or triple-delete the e-mail, depending on the sender's and recipients' e-mail program(s). The HAS staff member who reports the breach is responsible for notifying Department staff to delete the e-mail. The user is responsible for notifying all other recipients.
2. For a second offense of breach of confidentiality of CAREWare data:
  - a. HAS will notify the CAREWare user of the breach and the user will be locked out of CAREWare.
  - b. HAS will notify the user's supervisor and/or the executive administrator of the user's organization of the seriousness of this issue and require an acknowledgement by their

supervisor/administrator in writing. An e-mail to the HAS staff making the notification is acceptable written acknowledgement.

- c. HAS staff will report the breach to the section's Information Security and Privacy Coordinator, who will submit an Incident Report. Depending on the severity of the breach, the Incident Report will be sent to the division security officer or the Department's Inspector General for review.
  - d. If an electronic breach of confidentiality of CAREWare data is by unencrypted transmission via e-mail, the sender and all recipients will be instructed to double- or triple-deleted the e-mail, depending on the sender's and recipients' e-mail program(s). The HAS staff member who reports the breach is responsible for notifying Department staff to delete the e-mail. The user is responsible for notifying all other recipients.
  - e. If the supervisor/executive director wants the user to have access to the system after the second breach, the supervisor/executive director will send in a written request (e-mail is acceptable) to HAS asking that the user be granted access to CAREWare.
  - f. The incident will be reviewed by an internal HAS panel comprised of representatives of the division's information security officers, the HIV/AIDS Surveillance Unit and the HIV/AIDS Patient Care Community Programs Unit. The panel will meet at their earliest convenience and decide the appropriate remedy for the violation.
  - g. If the user or their organization disagrees with the decision of the panel, they may appeal the decision to the HAS administrator.
3. For a third or subsequent offense of breach of confidentiality of CAREWare data:
- a. HAS will notify the CAREWare user of the breach and the user will be **permanently** locked out of CAREWare.
  - b. HAS will notify the user's supervisor and/or the executive administrator of the user's organization and require an acknowledgement by their supervisor/administrator in writing. An e-mail to the HAS staff making the notification is acceptable written acknowledgement.
  - c. HAS staff will report the breach to the section's Information Security and Privacy Coordinator, who will submit an Incident Report. Depending on the severity of the breach, the Incident Report will be sent to the division security officer or the Department's Inspector General for review.
  - d. If an electronic breach of confidentiality of CAREWare data is by unencrypted transmission via e-mail, the sender and all recipients will be instructed to double- or triple-deleted the e-mail, depending on the sender's and recipients' e-mail program(s). The HAS staff member who reports the breach is responsible for notifying Department staff to delete the e-mail. The user is responsible for notifying all other recipients.
  - e. The user or their organization may appeal the permanent lock-out to the HAS administrator.