Security Incident Reporting

Intended Audience

- All ARIES Users
- Managers and Supervisors
- Administrative Agencies

Policy Background

All ARIES users are required to take all necessary steps to protect the confidentiality and security of the Protected Health Information (PHI) entered and stored in ARIES.

Examples of PHI contained in ARIES, which includes both primary and related/affected clients, are as follows:

- Client Name
- Client Telephone Numbers
- Client E-mail addresses
- Social Security Number
- Health Plan Beneficiary Number
- Client's Mother's Maiden Name
- Unencrypted Unique Record Number (URN)
- Client Address
- Client Fax Numbers
- Client Medical Record Number
- Date of Birth
- Account Numbers
- Client's Family Member's Name

Provider staff need to be aware of and follow their agency's guidelines pertaining to patient confidentiality and the Health Insurance Portability and Accountability Act (HIPAA).

Additionally, staff and agencies are required to report any breaches of security pertaining to PHI. A breach is defined as any failure to follow confidentiality protocols and procedures, whether or not PHI is actually released. The nature of the security breach – whether PHI was actually released or not – determines who to report the breach to and the timing required:

- Security incidents that do not release PHI should be reported to agency management as soon as possible (usually a person's direct supervisor).
- Security incidents that do release PHI must be immediately reported to (1) the user's agency management, (2) the agency's Administrative Agency (AA) (e.g., a local health department that contracts with the agency), and (3) the State Office of AIDS (OA).

Examples of security breaches that do not release PHI that should be reported to agency management are as follows: a compromised ARIES password, noticing that a user has posted his or her ARIES login and password where others can see it, a user walking away from his or her computer monitor with client information in view, ARIES-generated reports with PHI available where other staff can see them, etc.

Examples of breaches that do release PHI that need to be reported to the agency management, the AA (if applicable), and OA are as follows: accidental or intentional release of client information to the public or staff who have no business need to see the information (e.g., e-mailing a report with client names and addresses to staff outside the agency), inappropriate use of ARIES (e.g., users looking for ARIES information on acquaintances, friends, family, etc.), stolen or lost computer which was used to access ARIES (that might contain copies of ARIES reports with PHI), etc.

Procedures

To report a security incident to OA, call Dawn Munoz, Chief of OA's Data Systems Support Section, at 916-449-5891 or the ARIES System Administrator at 916-449-5842. In the event that neither of the aforementioned is available, leave a voicemail message and also send a brief e-mail regarding the incident to aries@cdph.ca.gov.

Compliance Monitoring

OA will evaluate all security incidents and may be required to report the incident to the CDPH Information Security Officer and CDPH Privacy Officer. OA will advise and assist agencies with incident reporting requirements and corrective action plans.

Additional Information

- For questions or clarifications regarding the reporting of ARIES security incidents, agencies should contact their AAs or Dawn Munoz, Chief of OA's Data Systems Support Section, at dawn.munoz@cdph.ca.gov.

Related Policies

- ARIES Policy Notice No. B2 regarding User Logins and Passwords
- ARIES Policy Notice B3 regarding Computer Workstations
- ARIES Policy Notice B4 regarding Mobile Devices
- ARIES Policy Notice F2 regarding the ARIES Help Desk (see "Procedures" section)
- ARIES Policy Notice G2 regarding ARIES Data Extraction