CLARK COUNTY
WASHINGTON

Health Insurance Portability and Accountability Act (HIPAA) Privacy Policy

Purpose

This policy is to ensure compliance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and its administrative regulations.

Scope

Clark County is a hybrid entity whose business activities include both covered and non-covered functions. This policy applies to all county departments and programs which perform health plan or health care provider activities that fall within the definition of a covered entity. The covered departments are Human Resources, Public Health, Community Services, Juvenile Court and the Sheriff's Office.

Definitions

1. **Protected Health Information (PHI)** is health information that is individually identifiable and relates to an individual's past, present or future physical or mental health or condition and related health care services, and is transmitted or maintained in any form or medium.
2. **Covered Entity** means a health plan, a health care clearinghouse, or a health care provider.
3. **Breach** is the acquisition, access, use or disclosure of PHI in a manner not permitted by law which compromises the security or privacy of PHI.

HIPAA Privacy Officer

The HIPAA Privacy Officer is designated by the Human Resources director and is responsible for:

1. Administering the county privacy policy.
2. Assisting covered departments with implementation of the privacy policy.
3. Investigating HIPAA complaints filed with the county and tracking complaints and resolutions.
4. Maintaining forms, tracking distribution of forms, and updating forms as needed.
5. Co-chair the county HIPAA advisory committee at periodic meetings, as needed.

6. Ensuring orientation training is conducted and documented for all new hires.
7. Ensuring covered departments provide and document appropriate training for staff who work with PHI.
8. Ensuring Notices of Privacy Practices for covered departments are distributed every three years or when significant revisions are made.
9. Reviewing and updating the privacy policy as needed to reflect changes to the law.
10. Ensuring appropriate responses to breaches and tracking reporting and resolution of breaches.

Administrative, Technical and Physical Safeguards

Clark County's covered departments and business associates shall ensure staff handling PHI comply with the following safeguards:

1. **Administrative Safeguards**
   - Report security breaches to supervisor or Privacy Officer immediately.
   - Properly dispose of PHI documents eligible for destruction.
   - Speak quietly when discussing client PHI so as not to be inadvertently overheard by others; avoid discussing PHI in public locations.
   - Verify fax numbers before sending document containing PHI; verify fax receipt.
   - Prevent incidental exposure of files and documents containing PHI by facing them away from colleagues and/or keeping such documents covered.
   - Store PHI in a locked desk drawer or cabinet when away from your desk.
   - Participate in HIPAA training as appropriate.
   - Ensure the proper Business Associate Agreements (BAAs) have been signed by entities the county contracts with to provide services that may have access to PHI.

2. **Technical Safeguards**
   - Keep passwords private; do not share or post them.
   - Use email encryption when transmitting PHI electronically to a recipient outside the county.
   - Comply with the County Electronic Communications Standards Policy

3. **Physical Safeguards**
   - Locate faxes, printers and copy machines in non-public areas.
   - Clear faxes, printers and copy machines of all documents containing PHI when finished with a job.
   - Limit access to PHI to authorized staff only.
   - Limit access to keys, magnetic cards and combinations to offices and storage.
   - Secure all storage areas containing PHI with locks.

Covered departments that keep electronic PHI (ePHI) also will comply with county HIPAA security policies and procedures.

Minimum Necessary Standards

Covered departments will make reasonable efforts to limit the use and disclosure of PHI to a minimum. Release of PHI will be only to accomplish the intended purpose of the use or disclosure. In general, this does not apply in the following circumstances:

1. Disclosure for treatment.
2. Disclosure to the subject of the information.
3. Use or disclosure made pursuant to an individual's authorization.
4. Disclosure made to U.S. Health and Human Services when information is required for enforcement purposes.
5. Use or disclosure as required by law or court order.
6. Use or disclosure required for compliance with the privacy regulation.

For appropriate uses, access to PHI will be provided on a need to know basis. Employees will access only information needed to accomplish a given function and only for the proper administration of an appropriate health-related program.

Training

1. Human Resources staff will provide basic HIPAA training to new members of the county workforce during new employee orientation and will obtain a signed Confidentiality of Health Information Agreement from each attendee.
2. Staff in covered departments will provide such training for new volunteers, temporary help, interns, contractors and students. Covered departments also will provide and document in-depth, comprehensive training for affected staff upon hire.
3. Refresher training will be provided by covered departments for affected staff annually, or as needed if policies and procedures change.

Breach Notification Process

Following a breach of unsecured PHI, notification will be provided as required by law.

Complaint Process

Any client or employee has the right to file a privacy complaint either directly with Clark County or with the Secretary of Health and Human Services, Office of Civil Rights, in Washington, D.C. The county will not require individuals to waive their rights as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

A complaint procedure is outlined in the county's Notice of Privacy Practices.

Employee Sanctions

Workforce members will access PHI only in accordance with their specific job functions. Appropriate sanctions will be applied to members who fail to comply with the privacy policies and procedures or with requirements of the federal regulation. The type of sanction will depend on factors such as the severity of the violation, whether the violation was intentional or unintentional, and whether the violation indicated a pattern of improper use or disclosure of PHI.

Covered departments, in consultation with the Privacy Officer, will:

1. Provide training to employees and document privacy procedures so expectations are clear.

2. Impose corrective action appropriate to the nature of the violation.
3. Comply with the county whistleblower policy.

No Retaliation

No covered component or county employee may intimidate, threaten, coerce, discriminate against or take other retaliatory action against any individual for the exercise by the individual of any right or process established by HIPAA privacy regulations, including filing a complaint.

No Waiver of Rights

No covered component or county employee may require any individual to waive their right to file a complaint with the secretary of the U.S. Department of Health and Human Services (HHS) as a condition of the provision of treatment, payment, enrollment in a health plan or eligibility for benefits.

Compliance Reviews

Representatives of the U.S. Department of Health and Human Services may conduct reviews of policies, procedures and practices to determine compliance with HIPAA Privacy requirements. Covered entity departments shall

- Work with the Privacy Officer during a review.
- Provide requested records and reports for investigators.
- Cooperate with the investigators.
- Permit access to facilities, books, records and accounts, including PHI, during normal business hours.

Dissemination of HIPAA Policies and Procedures

Clark County will maintain a copy of its HIPAA Privacy Policy on the county website and intranet site. Covered departments' Notice of Privacy Practices also are maintained on the county website.

Updated December 2017