CLARK COUNTY, NEVADA
HIPAA POLICIES AND PROCEDURES

Subject: **PRIVACY AND SECURITY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION**	POLICY NO: **HPMO-1** EFFECTIVE: 10/13
Distribution: Clark County Departments Designated as HIPAA Covered Components of the Hybrid Entity	Approved by: HIPAA Executive Steering Committee: 4/13 Don Burnette, County Manager: 10/13
Affects: All departments designated as components of Clark County's HIPAA Hybrid-Entity	Supersedes: Clark County Privacy Policies, effective 4/03, revised 12/06; Privacy of Individually Identifiable Health Information, effective date 12/06; Security of Electronic Protected Health Information, effective 12/06 Revised Date: 7/10, 7/13 Page 1 of 7

I. PURPOSE

To set forth the foundation for Clark County's compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[i], including the Modifications to the HIPAA Privacy, Security, Enforcement and Breach Notification Rules required by the Health Information Technology for Economic and Clinical Health Act (HITECH) regulations included in the American Recovery and Reinvestment Act (ARRA)[ii] of 2009, and the Genetic Information Nondiscrimination Act (Final Omnibus Rule) effective March 26, 2013[iii].

II. ORGANIZATIONS AFFECTED

All Clark County departments determined to be covered entities under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) are bound by this policy.

III. PROCEDURE

A. GENERAL

1. Clark County is designated a hybrid organization under HIPAA. As such, the County's covered departments are required to safeguard Protected Health Information (PHI), including electronic Protected Health Information (ePHI), in accordance with the regulations put into effect by the U.S. Department of Health and Human Services.
2. In regard to the authority for establishing, implementing, and enforcing the requirements of HIPAA and HITECH provisions at Clark County:
   a. The County Manager shall ensure that these policies are enforced, maintained and updated.
   b. Department Heads of covered departments are responsible for the development and implementation, training and enforcement of procedures to implement this policy at the departmental level. Department Heads shall appoint staff to serve as liaisons to the HIPAA Program Management Office.
   c. Department Managers are responsible for implementing security and privacy processes consistent with the criticality, value, and sensitivity of the information being handled.

Managers are also responsible for reporting individual complaints regarding privacy, and for administering corrective actions for workers known to be in violation of Clark County's privacy rules. Managers will designate the employees who will be responsible for receiving and processing requests from individuals regarding use and/or access to their protected health information (PHI).

d. The HIPAA Program Management Office will oversee a formal privacy and security compliance program and management structure responsible for investigating complaints and monitoring and maintaining security and confidentiality standards throughout Clark County. The HIPAA Program Management Office will conduct reviews and audits for adherence to this policy.

e. The County's Information Technology Security Administrator will oversee and provide guidance in the development and implementation of HIPAA required and addressable security requirements at the organizational level, investigate issues of non-compliance and disclosure, and provide recommendations for remedial actions.

f. Departmental liaisons designated by Department Heads shall be responsible for ensuring risk assessments and evaluations are conducted and appropriate procedures are developed, reviewed and revised as necessary.

g. Clark County employees, contractors, volunteers, students, and other temporary employees are responsible for understanding and complying with the policies addressed in this document. Violations of these policies may subject the violator to contractor sanctions or disciplinary actions in accordance with the applicable collective bargaining agreement, and may include termination and / or civil liability.

h. Questions or comments related to this policy should be directed to the Clark County Privacy Officer.

B. Clark County will maintain appropriate administrative, physical and technical safeguards to ensure privacy, integrity, confidentiality and availability of PHI.[iv]

1. Administrative Safeguards

a. Individual Privacy Rights. Covered departments will develop, implement and enforce procedures as appropriate to their covered entity designation:

1) Right to receive a Notice of Privacy Practices for PHI

2) Right to request restrictions of uses and disclosures of PHI

3) Right to request confidential communications for PHI

4) Right to request access PHI

5) Right to request to amend PHI

6) Right to an accounting of disclosures of PHI

7) Right to receive notice of a breach

b. Security Management

1) Risk Analysis (Required). All covered departments shall perform risk assessments for e-PHI within their purview.

i. Initial Risk assessments are immediately required for all new and existing systems and networks that create, process, store, or transmit e-PHI.

ii. Recurring risk assessment evaluations shall occur as part of the change management process, and where any standard or non-standard change will significantly affect the confidentiality, integrity, or availability of e-PHI.

iii. Both the initial and recurring risk assessments shall be completed using the OCTAVE™ Structured Risk Analysis process. Results of risk assessments shall be maintained by the covered department for a minimum of six years from the date of completion.

2) Risk Management (Required). Results of the risk assessments by covered departments are the basis for developing departmental policies and procedures and implementing security measures to reduce the exposure of e-PHI to malevolent, natural and technical vulnerabilities. Security measures shall be developed using the most current version of National Institute of Standards Publication 800-53, and its Consolidated Security Controls Baseline annexes, as a guideline.

3) Information System Activity (Required). Covered departments shall enable change auditing software on computer and network systems involved in the creation, processing, storage and transmission of e-PHI; and develop processes and procedures to ensure that audit logs, access reports and security incident tracking reports are reviewed on a regular basis.

c. Workforce security. All covered departments shall establish procedures that ensure only authorized personnel have access to systems that manage e-PHI.

1) Authorization and Supervision*. Ensure that procedures requiring managerial approval before any persons are granted access to computer or network systems that create, process, store or transmit e-PHI are developed, implemented, and maintained.

2) Workforce Clearance*. Ensure that background checks are performed where appropriate prior to any person being granted access to computer or network systems that create, process, store, or transmit e-PHI.

3) Termination*. Ensure that access to e-PHI is terminated when either the employment of a person ends, or the job responsibilities no longer warrant access.

d. Information Access Management. All covered departments shall establish procedures that ensure that computer systems and networks that create, process, store or transmit e-PHI have authorization controls in place that only allow authorized personnel access.

1) Access Authorization*. Ensure that workforce clearance and authorization is performed prior to granting workforce members access to e-PHI.

2) Access Establishment and Modification*. Ensure that access rights are evaluated for the workforce prior to granting access to computer systems and networks that create, process, store or transmit e-PHI; and re-evaluated when a workforce member's access requirements to e-PHI change. Modifications to the workforce member's access shall be properly authorized, and documented.

e. Training. Covered Departments shall ensure that all employees, contractors, volunteers, students and other temporary employees whose job responsibilities give them access to protected health information will receive awareness training about the policies, procedures and methods of safeguarding the security and confidentiality of PHI as part of their initial orientation. Additionally, Covered Departments shall provide detailed training about specific procedures developed to encompass their particular operations.

1) Covered departments will ensure all workers receive timely updates, changes to policies and procedures, and method of safeguarding the privacy and security of all forms of protected information.

2) Confidentiality Statements. Every person working in covered departments, including employees, physicians, contractors (temporaries, consultants, outsourcing agencies, etc.), students, and volunteers must understand Clark County's policies and procedures regarding the security and confidentiality of information, and must agree in writing to perform his or her work according to such policies and procedures.

3) Covered departments will retain documentation of training in accordance with the County's record management retention schedule for personnel files.

4) Security Awareness and Training.

i. Reminders*. The Covered department's e-PHI security liaison shall receive periodic security updates from the HIPAA Program Management office and the HIPAA Security Officer and disseminate the information to workforce members within their departments.

ii. Protection from Malicious Software*. Covered departments shall ensure that current software and security patches are applied to and enabled on computer and network devices that create, process, store and transmit e-PHI. Virus protection software, ad-ware and spy-ware software shall also be installed and activated.

iii. Log-In Monitoring*. Covered departments shall ensure that procedures for change auditing log monitoring are in place for the e-PHI security liaison to receive alerts notifying of failed computer system log-in attempts or unauthorized access to data files that contain e-PHI.

iv. Password Management*. Covered departments shall ensure that the following controls are in place where passwords are used.

1. Passwords must be at least eight (8) characters in length, include a varied set of numbers and symbols, and are not to be comprised of dictionary words or proper names.
2. Passwords must not be shared or written down and stored in insecure locations.
3. Passwords must be forced to be changed periodically, not to exceed 90 days and must be changed immediately if compromised.

f. Response and Reporting. All covered departments must develop response and reporting procedures to address security incidents and any breaches: oral or verbal; paper; or electronic (computer systems and networks) involving PHI. All known or potential breaches must be reported to the HIPAA Program Management Office immediately upon discovery.

g. Contingency Plan. All covered departments shall develop and test plans and procedures that can be implemented in the event of a malevolent, natural or technical disaster that damages computer systems or networks that process, store, and transmit e-PHI.

1) Data-backup Plan (Required). Data-backup plans for e-PHI adequate to restore e-PHI on the computer systems and networks where they are created, processed, stored, or transmitted.

2) Disaster Recovery Plan (Required). Disaster recovery plans and associated testing and revision procedures shall be implemented to facilitate the restoration of any e-PHI that may be lost in the event of a disaster.

3) Emergency Mode Operation Plan (Required). Downtime procedures shall be developed, tested, and maintained to both protect and facilitate access to e-PHI during emergency operations.

4) Testing and Revision *. Develop testing and revision procedures for data-backup plans, disaster recovery plans and emergency mode operation plans.

5) Application and Data Criticality Analysis *. Conduct a periodic application and data criticality or business impact analysis to assess the relatively criticality of HIPAA specific applications and data in support of the contingency plan components.

2. Physical Safeguards

a. Facility Access Controls. Each covered department will ensure that computer systems and networks that create, process, store or transmit e-PHI are kept in areas with physical security controls that restrict access to authorized, personnel, and approved physical and logical computer and network connections.

1) Contingency Operations *. Prepare in advance for each location a response plan that addresses the loss of access to computer and network systems and information due to planned or unplanned events. The preparations shall cover operations that allow facility access in support of the recovery and restoration of lost data when either the disaster recovery plan and/or the emergency mode operations plan has been activated.

2) Facility Security Plan *. For each location that creates, stores, processes or transmits e-PHI develop a Facility Security Plan that specifies protection requirements for the facilities, premises and equipment.

3) Access Control and Validation *. Develop and implement procedures to control and validate access for both employees and visitors to the covered department's work areas and/or facilities.

4) Maintenance Records *. Records of facility maintenance or maintenance to computer systems or networks that process, store, or transmit e-PHI shall be maintained.

b. Workstation Use. Each covered department shall ensure that only designated computer workstations enabled with appropriate physical and operating system software and application software security controls are used to access, process, store, and transmit e-PHI.

c. Workstation Security. Each covered department shall ensure that both physical operating system software and application software safeguards are in place to protect workstations that are used to access, process, store, and transmit e-PHI.

d. Device and Media Controls. Each covered department shall ensure that appropriate safeguards, processes and procedures are in place to govern the receipt, removal, storage, re-use and disposal of magnetic, optical or any other means of storing e-PHI.

1) Disposal (Required). Magnetic media shall be electronically overwritten prior to disposal. Optical media shall be physically destroyed when no longer used or no longer needed.

2) Media re-use (Required). Magnetic media shall be electronically overwritten before it is made immediately available for internal re-use.

3) Accountability *. Records regarding the installation, movement and removal of hardware and software used to create, process, store and transmit e-PHI shall be created and maintained using both the asset management process and configuration management database.

4) Data backup and storage *. A data backup and storage procedure shall be established and maintained that will allow for the retrieval of e-PHI.

3. Technical Safeguards

a. Access Control. Each covered department shall apply reasonable and appropriate access processes, procedures, and mechanisms to assure that only identified, validated and authorized individuals are granted access rights to e-PHI.

1) Unique User Identification (Required). Each individual user on Clark County networks shall be assigned a unique user name or ID number.

2) Emergency Access Procedures (Required). Emergency access procedures to support the retrieval of e-PHI during an emergency shall be developed.

3) Automatic Log-Off*. Configure computer systems and networks that create, process, store, or transmit e-PHI with mechanisms to terminate a session logon after a predetermined time of inactivity.

4) Encryption*. Apply encryption for data at rest and data in motion based on the results of the Risk Assessment. If encryption is applied to e-PHI it is considered "secure". Ensure that end-to-end encryption is used on or between computer

systems or networks not controlled by Clark County, where e-PHI is created, processes, stored, or transmitted.

b. Audit Controls. Each covered department shall install, configure, and implement change-auditing software on computer systems and network components that create, process, store, and transmit e-PHI.

c. Integrity. Each covered department shall ensure that computer systems and applications that process, store, or transmit e-PHI have the capability to maintain data integrity through one or more of the following: error-correcting memory, disk storage with built-in error detection and correction, checksums or encryption.

d. Person or entity authentication. Each covered department shall effect controls that verify that a person seeking access to e-PHI is the one claimed. Acceptable authentication measures for internal County access are username and password. Acceptable authentication for external access to e-PHI shall be enhanced with strong authentication – digital certificates, one-time passwords or both.

e. Transmission Security*. Each covered department shall effect controls that ensure that the integrity of e-PHI is maintained in transit via wire, cable, optical fiber, radio frequency and infrared in areas that are not under the County's control. Secure transmission mechanisms, such as Secure Shell, Secure Sockets Layer, and Transport Layer Security shall be used with Digital Certificates issued by a valid third party Certificate Authority (i.e., VeriSign, etc). The minimum cipher key strength and encryption algorithms that can be used are 128-bit AES.

4. Sanctions. Clark County will apply the appropriate sanctions against members of its workforce and business associates who fail to comply with Clark County's privacy and security policies. These sanctions include the disciplinary actions defined in the Clark County disciplinary process and the applicable collective bargaining agreement, as well as the remediation steps outlined in the Business Associate Agreement.

5. Mitigation. Clark County will mitigate, to the extent practicable, any harmful effect of a use or disclosure of PHI in violation of its privacy and security policies. Clark County is responsible to mitigate for harm caused by either members of the workforce or business associates.

6. Non-retaliation. Clark County will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual(s) for:

   a. Exercising any right under or participating in any process established by HIPAA's privacy rules (Title II, Part 164 Subpart E), including the filing of a complaint with Clark County or the Secretary of HHS;

   b. Testifying, assisting, or participating in and investigation, compliance review, proceeding, or hearing under part C of Title XI of the Social Security Act; or

   c. Opposing any act or practice made unlawful by HIPAA's privacy rules (Title II, Part 164 Subpart E), provided the individual has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve an improper disclosure of PHI.

7. Whistleblowers. Employees may use the compliance hotline to report suspected violations and breaches anonymously. Further information on protection for whistleblowers is located in Clark County Code section 2.38.040 (Appeal for reprisal or retaliatory action against county officer or employee who discloses improper governmental action).

8. Business Associate Contracts and Other Arrangements. Covered departments shall ensure that all consultants, vendors and other third parties who qualify as a business associate as defined by the HIPAA Rules [v] must sign and abide by Clark County's Business Associate Agreement.

9. Evaluation. Clark County and each covered department shall perform annual reviews to demonstrate its compliance with this policy. The reviews shall be presented to the HIPAA Program Management Office, and include remediation steps for any identified gaps in compliance with the policy.

10. Documentation. Clark County and covered departments will maintain adequate documentation for records related to the implementation of Clark County's privacy and security policies for six (6) years from the date of its creation or from the date when it was last in effect, whichever is later.

---

[i] Public Law 104-191, 45 CFR Parts 160, 162, and 164
[ii] Public Law 111-5
[iii] CFR Vol.78, No.17, Part II, Pages 5566-5702

[iv] Both required and addressable HIPAA Security Rule implementation specifications are included in this policy. Addressable implementation specifications are identified in this policy and are denoted by an asterisk (*).

1. Addressable implementation specifications provide Clark County and covered departments with some flexibility with respect to compliance and it must be determined whether an addressable implementation is reasonable and appropriate. The mechanism to determine reasonable and appropriate security measures will be the OCTAVE ™ Structured Risk Assessment and the resultant Risk Mitigation Strategy.

   The Risk Mitigation Strategy – the way that the department intends to address a risk through acceptance, mitigation with residual risk, or deferral -- shall be compared to the size, complexity, and capabilities of the department; the department's technical infrastructure, hardware, and software security capabilities; the cost of the security measures; and the probability and criticality of potential risks to electronic protected health information.

   Based on the above comparative analysis if a given addressable implementation specification is:

   a. Determined to be reasonable and appropriate, it must be implemented.

   b. Determined to be an inappropriate and/or unreasonable security measure, but the standard cannot be met without implementation of an additional security safeguard, an alternate measure that accomplishes the same end may be implemented.

   c. Not applicable – neither reasonable nor appropriate, and the standards can be met without implementation of an alternative measure in place of the addressable implementation specification, the decision to not implement – rationale, and how the standard will be met must be documented by the department head of the affected department and approved by the HIPAA Executive Steering Committee and the County Manager.

[v] §160.103 Business associate: a person who, on behalf of a covered entity or of an organized health care arrangement, in a capacity other than as a member of the covered entity's workforce, creates, receives, maintains, or transmits protected health information for a function or activity regulated by HIPAA, including claims processing or administration, data analysis, processing, or administration, utilization review, quality assurance, patient safety actitivies listed at 42 CFR 3.20, billing, benefit management, practice management and repricing; or provides, other than in the capacity of a workforce member, legal actuarial, accounting, consulting, data aggregation (as defined in §164.501, management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized healthcare arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.