Community Health Group	POLICY TYPE: ☒Corporate ☐ Divisional			
EFFECTIVE DATE: February 15, 2007	INITIAL APPROVAL DATE: 03/01/2009	NEXT REVIEW DATE: May 2017	POLICY NUMBER: 5501.1	
REVISION APPROVAL DATE: 02/007, 03/08, 03/09/, 01/10, 12/10, 3/11, 5/12, 9/13, 8/14, 11/14, 4/15, 4/16		APPLIES TO PRODUCT TYPE: ☒ CMC		PAGE: 1 of 7
POLICY APPLIES TO: All Divisions and Departments		CLASSIFICATION SERIES: Compliance		

SUBJECT:

Security Standards

Policy: It is the policy of Community Health Group (CHG) to provide the necessary means to protect the confidentiality and privacy of its members from unauthorized access to Individually Identifiable Health Information (IIHI) and Protected Health Information (PHI). Consequently, CHG has adopted standards of conduct and has implemented policies and procedures to ensure ongoing compliance with Health Insurance Portability and Accountability Act (HIPAA) and the Privacy Rule.

Purpose: The purpose of this policy is to ensure compliance with applicable HIPAA regulations and standards, and to ensure that CHG and its officers, employees, and agents have the necessary information to provide the highest quality access to medical care as possible while protecting the confidentiality of that information to the highest degree possible so that members do not fear to provide information to CHG and its officers, employees, and agents for purposes of obtaining health care services.

Procedure

As a California licensed health plan and Medicare Advantage sponsor contracted with CMS as a Medicare Advantage Part D Outpatient Prescription Drug Plan (MA-PD), CHG is responsible for ensuring the security of all communication transactions on behalf of its members, and associated with its operations. As a licensed health plan and MA-PD CHG's responsibilities include, and are not limited to receipt, processing, filing, storage, use and disclosure of Individually Identifiable Health Information and Protected Health Information as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the Privacy Rule.

The standards of conduct, policies, and procedures developed and adopted by CHG are predicated on the following standards.

Certification §142.308

- CHG shall adopt and implement all reasonable and necessary policies and procedures to enforce all applicable Certification requirements.
- CHG will undergo yearly internal evaluation.
- CHG will create a format for documentation of any inconsistencies, which will be promptly noted and corrected by the appropriate department(s).
- CHG shall develop and maintain a network schematic.

Chain of Trust Partner Agreement § 144.308(a)(2)

- CHG shall adopt and implement all reasonable and necessary policies and procedures to enforce all applicable Chain of Trust Agreement requirements.
- CHG shall have signed contracts with any organization that shares confidential electronic data.
- These contracts shall contain, but not be limited to:

    - Signatures of agreeing parties
    - Effective date, end date, and renew/review dates.
    - Definition of terms and conditions.
    - Procedures for reporting breaches.
    - Penalties for non-compliance.
    - Retention and destruction schedules.

- CHG and participating parties will keep an incident log to document any breaches. If CHG or any contracted party breaches, the other party will be notified and/or the incident log examined.

Contingency Plan § 142.308(a)(3)

1. CHG shall adopt and implement all reasonable and necessary policies and procedures to enforce the Contingency requirements.
2. CHG will create and maintain an inventory of all systems, support equipment and all voice and communication equipment with a list of all systems in order of priority.
3. CHG's Contingency Plan will be routinely updated to include, but limited to:
   a. Applications and Data Criticality Analysis-Assessment of sensitivity, vulnerability, and security of key information assets.
   b. Data backup plan that ensures the recovery of information that is lost or inaccessible.
   c. Disaster Recovery process that enables the restoration of systems and data following a catastrophic event.
   d. Testing and Revision during periodic updates and audits of all contingency plans.
   e. Emergency Mode Operation plan to ensure operation continuity for a period of time.

Formal Mechanisms for Processing Records §142.308(a)(4) (CA Civil Code 1798.85)

1. CHG shall adopt and implement all reasonable and necessary policies and procedures to enforce the formal mechanisms for Processing Records requirements.
2. CHG prohibits the posting, display, printing or use of Social Security numbers in any way, including in written correspondence to members, unless required by state or federal law.
3. CHG prohibits the use of Social Security numbers to access websites or any other electronic data systems.
4. The formal mechanisms for processing records will include, but not be limited to:
   a. Documented policies and procedures for the routine, and non-routine, receipt, manipulation, storage, dissemination, transmission, and/or disposal of health information.
   b. Differences between accountability of procedures for paper versus electronic media.

Information Access Control § 142.308 (a)(5)

1. CHG shall adopt and implement all reasonable and necessary policies and procedures to enforce the Information Access Control requirements.
2. CHG will have formal documented process for granting different levels of access to health care information, including an access authorization policy that establishes the guidelines for granting access to computers, transactions, programs, and processes and to what degree of access the user will be granted. The policy will include, but will not be limited to:
   a. Communication of the policy to all parties involved with access to health information
   b. On site and off site access
   c. Other means of access, including paper or voice
   d. Monitoring and enforcement of the policy
   e. Need to know basis for accountability
   f. Definition of authorization of requirements for various types of member data
   g. Process for termination of employees and monitoring of changing levels of access
   h. Approval, implementation and revocation of emergency access.

Internal Audit § 142.308(a)(6)

1. CHG shall adopt and implement all reasonable and necessary policies and procedures to enforce the Internal Audit requirements.
2. CHG shall have an in-house review of the records of system activity such as logins, file accesses, and security incidents.
3. CHG shall have internal processes for monitoring logins, files access, and security incidents, on a regular basis.

Personnel Security §142.308(a)(7)

1. CHG shall adopt and implement all reasonable and necessary policies and procedures to enforce the Personnel Security requirements.
2. CHG shall develop a process to ensure all personnel who have access to any sensitive information have the required authorities as well as all appropriate clearances. This shall include the following, but not limit:
   a. Supervising maintenance personnel.
   b. Maintaining records of access authorizations.
   c. Establishing personnel clearance procedures.
   d. Establishing and maintaining personnel security policies.
   e. Providing security awareness training.

Security Configuration Management § l42.308 (a)(8)

1. CHG shall adopt and implement all reasonable and necessary policies and procedures to enforce Security Configuration Management.
2. CHG shall have measures, practices, and procedures working in conjunction with other organizational measures, practices, and procedures that establish a coherent system of security. Included in these policies but not limited to:
   a. Documentation on hardware and software installation.
   b. Inventory of hardware and software assets.
   c. Maintenance review and testing for security testing.
   d. Security testing.
   e. Virus checking, testing, and response.

Security Incident Procedures §l42.308 (a)(9)

1. CHG shall adopt and implement all reasonable and necessary policies and procedures to enforce the Security Incident Procedures.
2. CHG shall have a formal process to identify, report and/or respond to real or potential violations of established security policies. Items included, but not limited to:
   a. Definition of serious and non-serious incident
   b. Handling of viruses; who investigates different levels of virus incidents
   c. Timelines for investigating and reporting, and recommending corrective action and implementing disciplinary actions
   d. Coordination with local and federal law enforcement
   e. Standards for anti-virus software, intrusion detection software, and network software

Security Management Processes §l42.308(a) (10)

1. CHG shall adopt and implement all reasonable and necessary policies and procedures to enforce the Security Management Processes.
2. CHG shall have comprehensive process to ensure the prevention, detection, containment, and correction of security breaches. Involving risk analysis and risk management, it will include, but not be limited to:
   a. Establishment of accountability.
   b. Management controls policies and education.
   c. Electronic controls.
   d. Physical security.
   e. Sanctions for the abuse and misuse of its assets both physical and electronic.
   f. Documented security policy.

Termination Procedures §142.308(a)(I1)

1. CHG shall adopt and implement all reasonable and necessary policies and procedures to endorse all applicable termination procedures.
2. CHG will implement a termination process that includes a user's internal and external access and identifies/acts upon potential security concerns for the ending of an employee's employment, agents or contractors user access. These procedures are important to prevent the possibility of unauthorized access to secure data by those who are no longer authorized to access the data.
3. Termination procedures would include the following implementation procedures:
   a. Combination/Key locks changed- Combination/key locks will be changed both on a recurring basis and when job responsibilities change or termination from employment.
   b. Removal from access lists-eradicating a person's (employee, temporary, contractor, external agent) access privileges upon the release from responsibilities or the termination of employment.
   c. Removal of user accounts.
   d. Turn in keys, token or cards that allow access-all access devices (keys, tokens, access cards, etc) retrieved from persons when job responsibilities change or termination from employment occurs.

Training §142.308(a)(I2)

1. CHG shall adopt and implement all reasonable and necessary policies and procedures to endorse all applicable training requirements.
2. CHG will provide security training for all staff regarding the vulnerabilities of the health information in an entity's possession.
3. CHG will instruct all employees regarding compliance and consequences of failure to do so.
4. The implementation features are as follows and not limited to:
   a. Awareness Training for all Personnel.
   b. Periodic Security Reminders.
   c. User education concerning virus protection.
   d. User instruction regarding importance and use of monitoring log, and how to report discrepancies.
   e. User education regarding password management.

5. Security Awareness training and virus training programs will be provided for all employees, agents, and contractors on an ongoing basis to include periodic reminders and as job responsibilities change. Also, provide training regarding the identification and reporting of unusual system activities that may indicate security breaches will be provided.

Physical Safeguards for Data Integrity, Confidentiality and Availability § 142.308(B)

1. CHG shall adopt and implement all reasonable and necessary policies and procedures to endorse all applicable physical safeguards for data integrity, confidentiality and availability.
2. CHG shall adopt and implement all reasonable and necessary policies and procedures to endorse all applicable assigned security responsibility.
3. CHG will assign the security responsibility to a specific individual or organization and the assignment must be documented. Responsibilities include:
   a. Use of established security measures to control and secure data
   b. The conduct of personnel in relation to the protection of data

Media Controls §I42.308(b)(2)

1. CHG shall adopt and implement all reasonable and necessary policies and procedures to endorse all applicable media controls.
2. CHG will establish media controls in the form of formal, documented policies and procedures governing the receipt and removal of hardware/software such as diskette and tapes into and out of facility. Mandatory implementation features include:
   a. Access Control- Access to areas where media is stored must be limited to authorized employees, agents or contractors. All equipment, hardware, software and electronic storage media must be accounted for and maintained ensuring all systems, including applications and databases are appropriately backed up, marking, safeguarding, handling, and disposing of confidential or sensitive data and reports.
   b. Accountability.
   c. Data Backup.
   d. Data Storage.
   e. Disposal - ensure that the information on the media has been removed. Controlled access media may be locked in a secure environment.

Physical Access Controls §I42.308(b)(3)

1. CHG shall adopt and implement all reasonable and necessary policies and procedures to endorse all applicable physical access controls.
2. CHG will establish formal, documented policies and procedures for limiting physical access while ensuring proper access to premises and facilities. Mandatory implementation features included:
   a. Disaster Recovery-The disaster recovery plan will include the procedures to restore loss of data and to continue operating in the event of fire, vandalism, natural disaster, or system failures.
   b. Emergency Mode Operation.
   c. Equipment Control-Equipment and access to equipment will be recorded.
   d. Facility Security Plan.
   e. Procedures for Verifying Access authorizations before Granting Physical Access- Ensure that access to sensitive information handling areas is physically restricted only to authorized personnel (locked doors, guards). Safeguard to ensure production and test environments are segregated and restrict physical access to authorized personnel.
   f. Maintenance Records- Policy will address the need for physical security, safety and protection of data premise and facilities Record and maintain a record of repairs, maintenance and modification to the physical components of the facility.
   g. Need-to-know Procedures for Personnel Access -Access privileges of employees, agents and contractors will be validated before granting privileges, and safeguards will be in place regarding the use of keys, cards, or badges to control access to restricted areas.
   h. Procedures to Sign in Visitors and Provide Escorts.
   i. Testing and Revisions.

Policy/Guideline on Workstation Use-Physical Security §I42.308(b)(4)

1. CHG shall adopt and implement all reasonable and necessary policies/guidelines on workstation use.
2. CHG will establish physical safeguards to eliminate or minimize the possibility of unauthorized access to information. This will apply to public buildings, provider offices and in areas where there is heavy pedestrian traffic.
3. Requirements will be to place monitors in such a manner where the general public cannot view the screen contents. Additionally, screen savers should be employed. There should be limited access to the following areas:
   a. Building
   b. Office
   c. Workstation
   d. Systems
   e. Printers and faxes
   f. Printed reports
   g. Downloaded data
   h. Removable media
   i. Remote devices
   j. Medical record storage areas.

Secure Workstation Location-Physical Security §l42.308(b)(5)

1. CHG shall adopt and implement all reasonable and necessary policies and procedures to endorse all applicable secure workstation location requirements. Policy will address the following areas:
   a. Granting access only to named resources.
   b. Discourage unauthorized access via signage.
   c. Ensure secondary exits are locked to prevent outside entry.
   d. Ensure all workstations are protected from unauthorized use and view (screen savers, passwords, and monitor positioning.
   e. Limit accessibility to printed material by restricting proximity to unauthorized personnel.
   f. Ensure systems have the ability to define user or role based accessibility.
   g. Encryption and compression of downloaded data as user need arises.
   h. Copying of data should not be permitted unless the user's role requires it.
   i. All backups must be kept locked in a designated area.
   j. Mechanisms must be used to report incidents where security or privacy issues may have been violated, e.g. worksheet placed in appropriate section of the security manual.

Security Access Training-Physical Security §142.308(b)(6)

1. CHG shall adopt and implement all reasonable and necessary policies and procedures to endorse all applicable security awareness training.
2. CHG will establish security awareness training for all employees, agents and contractors. This training shall be conducted at initial orientation for new personnel as well as on-going training. Training should be conducted, at a minimum, annually and should reflect the following guidelines:
   a. Establish periodic reminders via e-mails, bulletin boards, posters, Intranet, etc.
   b. Use visual reminders at a central location to reinforce best practices.
   c. Record attendance.
   d. Establish disciplinary actions following a security breach.

Technical Security Mechanisms (Network Security) Communication and Network Controls § 142.308(d)(1)

1. CHG shall adopt and implement all reasonable and necessary policies and procedures to enforce all Network Controls.
2. CHG will protect data being transmitted electronically over open networks by ensuring that data is not easily intercepted and interpreted by parties other than the intended recipient, and to protect information systems from intruders attempting to access systems through external points.

3. CHG shall use a combination of controls to protect the data:
   a. Integrity Controls
   b. Message Authentication Code
   c. Access Controls
   d. Encryptions

4. CHG will implement the following features to ensure data cannot be easily intercepted and interpreted by parties other than the intended.
   a. Alarm
   b. Audit Trail
   c. Entity Authentication
   d. Event Reporting

Access Privileges: ☒ All ☐ _____

Regulatory: CMS: _____

NCQA:

Attachments: None

Policy Status: ☒ Signed (Signature on File) ☐ Active Draft ☐ Policy in Development

Approved By: Signature: _____

Department Head: Chief Compliance & Regulatory Affairs Officer

Date: _____

Signature: _____

Division Chief: Chief Executive Officer

Date: _____