Close This Window

Policy: ADMIN: Information Security and Privacy Policy
Version: 3
Location: Information Management /
Sponsor: Director, Security & Computer Operations
Department: Administrative Manual; Privacy / Compliance
Organizations: CDHealth (Corporate), CDH, Convenient Care, CNS, CDPG, Wyndemere, Westbridge, Wynscape
Date of Last Review:
Date of Last Revision: 02/04/2005

I. PURPOSE:

This policy identifies information security and privacy requirements for the processing, storage, and handling of information at Central DuPage Health. Objectives of this policy are to ensure that information related to patient treatment, payment, or operations is protected, that patients' legal rights are protected, and that information operations remain in compliance with local, state, and federal statutes and regulations as well as business needs.

Central DuPage Health will audit automated information and voice systems and adherence to privacy practices on a periodic basis to ensure compliance with this policy. Information systems users should be aware that there is no expectation of personal privacy while using Central DuPage Health information systems and resources and that data can be viewed, audited, or removed at any time by the organization.

Violation of this policy may result in a denial of access to Central DuPage Health information and disciplinary actions may be considered up to and including termination of employment or the relationship with Central DuPage Health.

Personnel who are not employees of Central DuPage Health will indemnify, hold harmless and defend (if so requested by Central DuPage Health) Central DuPage Health and its officers, directors, affiliates and members from and against any and all liabilities, costs, expense and damages, including attorneys' fees, actually and necessary incurred arising out of a breach or violation of this policy as well as any other of the organization's policies or procedures requiring privacy and confidentially. In the event that potentially illegal activities are conducted using Central DuPage Health information resources, the organization will work with the appropriate law enforcement agencies to investigate and prosecute the activity in question.

Scope: Central DuPage Health protects patients' rights to privacy and confidentiality by creating and putting into practice policies and procedures that allow access to Protected Health Information (PHI) only for legitimate reasons, such as, treatment, payment, or operations. Employees must secure this information in a way that protects the privacy of our patients at all times, regardless of how the information is stored or processed.

This policy applies to all health system member organizations and includes, but is not limited to employees (full-time, part-time, temporary, reserve, and in-house registry), medical staff, vendors, consultants, contract workers, patients, students, interns, visitors, volunteers and employee family members. An Acknowledgement Statement (Attachment 1) will be signed by all personnel prior to gaining access to information managed by Central DuPage Health. This policy also applies to all equipment that is owned, leased, or maintained by the organization, including equipment that is located in an individual's home, and covers equipment used in facilities that are owned and leased by the organization. This policy applies to all types of information generated, used, or held by Central DuPage Health that is used within the scope of the organization's business processes in all formats, including electronic, magnetic, paper, or other.

Information systems and other computing devices include all components connected or related to the Central DuPage Health computer network and telecommunications environment, including, but not limited t Internet, intranet, remote access, e-mail, workstations, Personal Digital Assistants (PDA), removable media, telephones, and other related computing equipment.

II. POLICY STATEMENT

Access controls will be established for all information systems and facilities in accordance with the HIPAA Security Rule. The types of controls may vary but must, at a minimum, be consistent with this policy and include a means to identify and authenticate the user. Access controls will be established commensurate to the sensitivity of the information processed or stored by the system. User accounts on information systems are restricted to the assigned user and must be authorized by the user's immediate supervisor. Sharing of assigned account privileges and access controls (e.g., passwords, tokens, and badges) is not permitted, except in the case of an emergency. If a password is shared for any reason, it must be changed immediately after the need for a shared password has ended. Access to any Central DuPage Health information system may be modified or revoked at any time by the organization.

The need-to-know principle will be applied in granting information access. This principle requires that information only be provided to individuals that require the information to carry out their duties. Users may not attempt to gain excessive privileges in an unauthorized manner beyond what they are assigned.

Information systems that are provided specifically in direct support of patient care or that are located in clinical areas (including bio-medical, telemetry, and/or administrative systems) may not be used for personal use at any time.

Information systems that are administrative in nature, that are not used to support direct patient-care, and that are located in non-clinical areas must be dedicated for business use, research, or other support functions. The unit supervisor may approve limited occasional personal use of these systems, as needed for activities, such as on-line travel reservations, news, financial updates, and web-based e-mail, as long as use is not excessive. The unit supervisor shall determine excessive use guidelines.

It is prohibited to intentionally use Central DuPage Health information systems for activities that are considered illegal, obscene, defamatory, or which are intended to harass or intimidate another person. The organization's information systems will not be used to damage or impair the operations of other systems of any type, regardless of whether at a Central DuPage Health facility, or some other entity. Also, at no time will Central DuPage Health information systems be used to support a personal business or some other activity for personal gain. Activities that may degrade internal systems operations, or affect work productivity, are also prohibited. Examples of such activities, include: accessing, or downloading games, installing personal software, sending chain letters, installing peer-peer file sharing tools (e.g., MP3 sharing tools), listening to radio stations or on-line music, emails related to gambling or betting pools.

Unauthorized duplication of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Central DuPage Health or the end user does not have an active license, is strictly prohibited.

At any alternative work sites, which may include employee and physician home offices, physician practice offices, patient homes, etc., precautions must be taken to protect Central DuPage Health information, hardware, and software from theft, damage, and misuse. Information must be protected in a manner commensurate with its sensitivity, value, and criticality. When accessing the organization's network from a remote site, or when using mobile devices (such as a PDA or laptop), the user assumes responsibility for the security of the information that is stored and processed by the device.

Central DuPage Health equipment that is located at a remote site or home office must be returned to the organization at the termination of the relationship with Central DuPage Health. Personal computing equipment may be used to connect to the Central DuPage Health network only for the conduct of business and operations from a remote site, such as a home office. Personal computers must, at a minimum, have the most current and up-to-date anti-virus and personal firewall software installed.

Personal computing devices that have been used to store and process protected health information (PHI) must be sanitized when no longer used or when the user's employment or medical staff privileges at Central DuPage Health ends. Methods of sanitization may be obtained from the Telecommunications and Information Services (TIS) department. Further, upon termination of employment or medical staff privileges, all PHI will be returned to the organization and no copies will be retained. All materials that contain PHI created on behalf of Central DuPage Health remain the property of the organization.

Media storage that is no longer required for use and that has been used to record sensitive or protected health information must be destroyed using approved destruction methods. Shredding is an approved destruction method for paper. Magnetic media and CD's often have special destruction methods and users should contact the CDH computer help desk at 630-933-2639 for guidance on destruction methods.

In general, e-mail communications between a provider or physician and their patients is permitted if it is mutually agreed upon with the patient affected. It is the responsibility of the individual to use professional judgment in assuring that such transmissions are authorized. A signed authorization will be obtained from the patient prior to conducting communications by e-mail directly to the patient. Physicians may also receive e-mail distribution of patient-related reports containing PHI only after authorization by the Medical Staff Office and validation of active e-mail accounts.

Central DuPage Health has put in place policies regarding access to medical records by staff and employees and has carefully outlined the circumstances under which a patient's PHI may be released to parties outside the hospital or physician practice. When using or disclosing PHI or when requesting PHI from another Central DuPage Health entity, personnel will make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. Written consent will be obtained, as required, prior to releasing any document that contains PHI (Attachment 2 - Authorization for Release of Medical Information).

A patient has the right to confidential communications and a right to restrict disclosures of information related to communications made by Central DuPage Health to the patient, by allowing the patient to request that such communications be made to the person at an alternative location or by alternative means.

Further, the patient, or anyone to whom the patient has given written permission, or the patient's legal representatives, has the

right to read or obtain a copy of a patient's PHI. A patient has the right to access an accounting of disclosures of their PHI and to request an amendment to their medical record. If requested by the patient or the patient's personal representative, an accounting of disclosures must be provided to the patient. As required by the privacy law, the accounting will detail PHI that has been forwarded to third parties.

For additional information related to a patient's rights to confidential communications, accounting of disclosures, amendment of PHI or right to access, please refer to the Privacy Standard. The Privacy Standard contains the necessary protocols to follow related to processing patient PHI in accordance with the HIPAA Privacy regulation.

IV. Contact Information

If you have questions regarding this policy or require additional information regarding Information Security or Privacy at Central DuPage Health, please contact the individuals as follows:

Justine Dover, Director and Privacy/Compliance Officer, may be reached at (630) 933-5157; or
Andy Reeder, Director and Information Security Officer, may be reached at (630) 933-2639

ORIGINAL DATE: 02/01/2004

END

- Signature On File -

Back To The Top