Security Awareness for Protected Health Information (PHI)

- All new hospital employees and associates must receive appropriate security training before being provided with access or accounts on the hospital's information systems.

- Your initial username/password will be provided to you at the time of training by your trainer who will guide you through the log on process. The first time that you log into the new system a prompt will show that your password has expired. Type in your username as your OLD password. Enter your NEW unique password. Your password must be at least 6 characters. You will need to retype your new password a second time for verification.

- Users are locked out of the system after three unsuccessful attempts. Contact the Information System HELP desk for assistance, outside the hospital call 304-526-2626 or from within the hospital extension 2626 with problems logging into the new system. After hours, follow this same process outlined, the caller may be prompted to leave name and number for a return call from the on-call person.

- At a minimum, the hospital's password management system must:
  - Require the use of individual passwords to maintain accountability.
  - Where appropriate, allow workforce members to select and change their own passwords.
  - Require unique passwords that meet the standards defined by the Information Security Officer.
  - Require regular password changes (at least every 180 days for designated systems).
  - Not display passwords in clear text when they are being input into an application.
  - Require the storage of passwords in encrypted form using a one-way encryption algorithm.
  - Require passwords to be given to users in a secure manner.
  - Require the changing of default vendor passwords following installation of software.

- The hospital's password creation standards require strong passwords creations that have these characteristics:
  - Password must have a minimum length of six characters, eight characters recommended.
  - Passwords must not be based on something that can be easily guessed or obtained using personal information (examples: names, favorite sports team, etc.).
  - Contain both upper and lower case characters (example, a-z, A-Z).
  - Have numbers and punctuation characters as well as alphabetical characters (example: 09!@%&*aB+-=)
  - Are at least eight alphanumeric characters long.
  - Are not words in any language, slang, dialect, jargon, etc.
  - Are not based on personal information, names of family, etc.
  - Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmlB1w2R!" or some variation.

- Poor, weak passwords have the following characteristics:
  - The password contains less than eight characters.
  - The password is a word found in a dictionary (English or foreign).
  - The password is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - The words "Cabell Huntington Hospital", "sanjose", "sanfran" or any derivation.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aabbb, qwerty, zyxwvs, 123321, etc.
    - Any of the above spelled backwards.
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret).

**NOTE:** Please do not use any of these examples as passwords!

Revised 12/11 ke
Security Awareness for Protected Health Information (PHI)

Password Protection Standards: Do not use the same password for Cabell Huntington Hospital accounts as for other non-Cabell Huntington Hospital access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don’t use the same password for various Cabell Huntington Hospital access needs. For example, select one password for the Engineering systems and a separate password for IT systems. Select a separate password to be used for an NT account and a UNIX account.

Do not share Cabell Huntington Hospital passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential Cabell Huntington Hospital information. You will be held responsible for all access to Hospital systems using your password.

- At a minimum, hospital password management training and awareness must involve requirements for use of information systems including, but not limited to:
  - The importance of keeping passwords confidential and not sharing them with those that ask
  - The need to avoid maintaining a paper record of passwords, unless the record can be securely stored
  - Changing passwords whenever there is any indication of possible information system or password compromise
  - The hospital’s password standards
  - The importance of changing passwords at regular intervals and avoid re-using old passwords
  - Changing temporary passwords at the first log-on
  - Not including passwords in any automated log-on process (example: stored in a macro or function key)
  - Ensuring that hospital workforce members understand that all activities involving their user identification and password will be attributed to them

Here is a list of “do not’s”:
- Do not reveal a password over the phone to ANYONE
- Do not reveal a password in an email message
- Do not reveal a password to the boss
- Do not talk about a password in front of others
- Do not hint at the format of a password (e.g., “my family name”)
- Do not reveal a password on questionnaires or security forms
- Do not share a password with family members
- Do not reveal a password to co-workers while on vacation

Termination of Access Enforcement: Any employee found to have violated this policy will be subject to disciplinary action as defined in the Disciplinary Policy, Policy V-30

Security Breach: It is the policy of Cabell Huntington Hospital to properly investigate and, where required, notify the appropriate individuals and organizations in the event of a breach involving unsecured protected health information (“PHI”)

Policies and Information: For more in-depth information, but not limited to these, regarding policies and procedures related to security awareness of PHI view the following documents on the hospital intranet (www.chh.org): under policies & manuals:

- Administrative Policy Manual
  - Policy 1 - 33A: Password Selection and Security
  - Policy VI - 1: Minimum Necessary Standard
  - Policy VI - 2: Accounting and Tracking Disclosures of Protected Health Information
  - Policy VI - 3: Amendment of protected Health Information by Patients or their Representatives
  - Policy VI - 4: Designated Record Set
  - Policy VI - 5: Security Breach Investigation and Notification

- HIPAA Information
  - Security Standards Final Rule Standards of Privacy
  - HIPAA Privacy
  - HIPAA Seminar Outline
  - QS HIPAA Guide
  - Federal Register Privacy Rules (all numbers)

- CHH IS Policies
  - Policy 3 - Workstation Security
  - Policy 4 - Information Access Management Access Establishment and Modification
  - Policy 5 - Security Awareness and Training