Policy Number:	**8.17**	**Original Date Issued:**	April 9, 2004
Section:	Information Management	**Date Reviewed:**	May 22, 2014
Title:	Password Management	**Date Revised:**	May 22, 2014
Regulatory Agency:	**HHS**		

I. PURPOSE:

The purpose of the Password Management Policy is to establish Children's standards and guidelines for the creation of strong passwords, the frequency of password changes, and management and protection of those passwords.

II. SCOPE:

This policy applies to all Users who have or are responsible for an account on any system that resides at any Children's facility, has access to the Children's network, or stores any Children's information and their passwords.

The Policy and Standard do not apply to passwords used to protect individual documents, but the Guideline does apply to all passwords including those used to protect individual documents.

The Policy, Standard and Guideline do not apply to passwords used for personal accounts that do not create, receive, maintain or transmit Children's data.

The HIPAA Security Regulation, Section 45 CFR 164.308 5(i)(ii)(D), Implementation Specification for Password Management Standard, requires Children's to provide *"Procedures for creating, changing, and safeguarding passwords."*

III. DEFINITIONS:

Definitions can be found in the Children's *Information Security Policies Glossary of Terms* document.

IV. POLICY:

1. Passwords should be one component of the Login Credentials used to verify a Users' identity when obtaining access to Children's Resources including electronic Protected Health Information (ePHI).

2. Users must change their passwords at least once every one hundred twenty (120) days.

3. Users must change any temporarily assigned passwords at initial login.

4. Users must contact the Solution Center and verify their identity to have an account reactivated or password reset. Users may not have their managers, co-workers or direct reports contact the Solution Center on their behalf.

5. Users must immediately change their Children's password(s) if there is reason to believe their account or computer system is compromised, meaning that someone else may have unauthorized access to their account or computer system. (Indications of this include disappearing files or emails, selecting and clicking a URL within a suspicious email, or other suspicious activity). Users must also contact the Solution Center if they believe their account or computer system is compromised.

6. Users must not share their Children's password with anyone, including administrative or executive assistants and the Solution Center, in any manner. All passwords are to be treated as confidential Children's information.

7. Users must not write down their password(s) (e.g., by writing the password on a sticky note) or store their password electronically without encryption. Note that password-protected Excel or Word files can be encrypted in some versions but they can typically be easily hacked. As an alternative, please refer to the Password Storage Vault Standard for allowed password storage vaults.

8. System administrator passwords (e.g., Windows Administrator, application administrator accounts) must be changed every ninety (90) days.

9. User accounts that have system administrator access granted through group memberships or application accounts must have a password that is unique from all other accounts held by that user.

10. System administrators are responsible for changing administrator passwords. System administrators may not have their direct reports or non-administrator level users change passwords on their behalf.

11. System administrators must immediately change the administrator password if there is reason to believe that the administrator account or computer system may be compromised.

12. Unencrypted passwords must not be included within URL bookmarks, automated applications or scripts.

13. Patient and patient family passwords used on Children’s systems (such as for MyChart) are not required to change their passwords again after they initially set a new password during their first login.

14. All Users must conform to the *Password Management Standard* and refer to the *Password Management Guidelines* listed below.

V. PASSWORD STANDARD:

These standards may change periodically but are up-to-date as of this document's publication date.

Passwords for access to the Children's network and computer systems must meet the following requirements:

1. All passwords must be associated back to a valid Children's account.

2. Passwords must contain a minimum of eight characters. If the system does not support a minimum of eight characters, the password must meet the maximum length criteria for that system.

3. Passwords must contain at least three of the following four character types:

    a. Uppercase alphabetic characters (e.g., A-Z)

    b. Lowercase alphabetic characters (e.g., a-z)

    c. Numbers (e.g., 0-9)

    d. Special characters or punctuation (e.g., ~!@#*^&%+()=_-)

4. Users should create a password or passphrase that is used solely for Children's purposes and not the same as the password used for online banking, credit cards, other personal, or non-Children's business accounts.

5. Users may not re-use any of the last five (5) passwords that they have previously used. Minimum password age is 1 day.

6. Passwords must not spell a word with a number added to the beginning or the end such as "1Prime3".

7. Passwords must not be "hard-coded" in any automated login process or script. The exception to this requirement is our approved single sign-on tool, Caradigm (formerly Sentillion) Vergence.

8. Passwords must not be stored or transmitted in plain text; encryption must be used at all times.

9. User accounts will become locked after 6 unsuccessful login attempts using incorrect passwords.

10. User accounts that become locked will remain locked based on the following schedule, provided that the underlying system can support the tiered lockout:
    a. 1st lockout = 15 minute duration
    b. 2nd lockout = 30 minute duration
    c. 3rd lockout and beyond = add 15 minutes to prior duration

VI. PASSWORD GUIDELINES:

These guidelines may change periodically but are up-to-date as of this documents' publication date.

1. Users should follow these password Guidelines :
    a. Avoid reusing a previously used password.
    b. Do not use automatic logon functionality (e.g., the "Remember Password" feature provided in most search engines, web browsers and web sites).
    c. Create a hard-to-guess but easy-to-remember password by using a passphrase. Type the entire phrase (some applications and websites let you use spaces) or use the initials of each word in the phrase (for instance, "At Children's we are Dedicated to all Better!" would be "ACwaD2aB!" or "I graduated from Lincoln Elementary School in '85" would be "IgfLESi85".
    d. Use two or three short words that are unrelated and replace some letters with numbers "L@ughingC0wSyr1nge".
    e. If you use common words that exist in the dictionary, deliberately misspell those words to avoid password guessing by malicious users.
    f. Passwords must not be easily guessable such as:
        - Words that appear in the dictionary such as "DOG" or "Briefcase".
        - Derivatives of User IDs such as a password of 110785abc for a User ID of 110785.
        - Common character sequences such as "123456" or "QWERTY".
        - Birthdays or personal information such as addresses, phone numbers, license plates, pet names, family member names, friend names, etc.
        - Parts of speech, for example, Geographical locations such as "Atlanta", common acronyms such as "CHOA", or slang.

2. Users responsible for the provisioning and support of User accounts should follow these password Guidelines:

    a. Do not use Sensitive Information for initial (i.e., "first-time") or reset (i.e., "one-time") passwords (e.g. part or all of a social security number or date of birth).

    b. Do not use the same "first-time" or "one-time" password for all users.

    c. Always verify a User's identity before resetting a password.

    d. Never ask for a User's password.

3. Users responsible for the design and implementation of systems and applications should follow these password Guidelines:

    a. Change default and vendor account passwords.

    b. Passwords should support authentication of Users, not groups of Users.

    c. Implement strict controls for administrator level and shared account passwords.

    d. Do not use the same password for multiple administrator accounts.

    e. Do not store passwords in easily readable form (e.g., stored or transmitted using weak encryption).

    f. Implement automated notification to the User when a password is changed or reset.

VII. EXCEPTIONS:

Exceptions to this Policy must be reviewed and approved in writing in accordance with the *Information Security Policy Exception Procedure*. All approved policy exceptions will be reviewed periodically for appropriateness and may be revoked at any time by notifying appropriate personnel per the *Information Security Policy Exception Procedure*.

VIII. POLICY REVIEW:

This policy will be reviewed and updated as needed, at least once a year or as required by law or relevant regulation. When reviewed, the policy will be evaluated to determine its effectiveness in complying with key regulations such as the HIPAA Security Rule, as well as in meeting Children's evolving operational needs.

In accordance with the Code of Federal Regulations, 45 C.F.R. 164.306(b)(2)(i), all iterations of this Policy will be retained for a minimum of 6 years.

IX. POLICY AUTHORITY/ENFORCEMENT:

The Children's designated Information Security Officer has general responsibility for implementation of this policy.

Violations of this policy may result in suspension or loss of the violator's use privileges, with respect to Children's Resources, and/or disciplinary action. Access privileges may be restored only after consultation between the designated Information Security Officer and Children's Management and/or Children's Senior Management personnel.

Anyone who knows or has reason to believe that another person has violated this policy should report the matter promptly to his or her supervisor; or report to the Compliance Connection Hotline at 1-877-373-0126, or online at https://choa.alertline.com. All reported matters will be investigated, and, where appropriate, steps will be taken to remedy the situation. Where possible, Children's will make every effort to handle the reported matter confidentially. Any attempt to retaliate against a person for reporting a violation of this policy will itself be considered a violation of this policy is strictly prohibited and will result in disciplinary action.