



**CENTERS for MEDICARE & MEDICAID SERVICES**

Enterprise Information Security Group

7500 Security Boulevard

Baltimore, Maryland 21244-1850



**Risk Management Handbook**

**Volume III**

**Standard 4.3**

**Non-Standard Account Authenticator  
Management**

**FINAL**

**Version 1.0**

**October 30, 2013**

Document Number: CMS-CISO-2013-vIII-std4.3

**(This Page Intentionally Blank)**

**SUMMARY OF CHANGES IN *NON-STANDARD ACCOUNT AUTHENTICATOR  
MANAGEMENT, VERSION 1.0***

1. Baseline Version.

**(This Page Intentionally Blank)**

**TABLE OF CONTENTS**

<b>1</b>	<b>BACKGROUND .....</b>	<b>1</b>
<b>2</b>	<b>PURPOSE.....</b>	<b>1</b>
<b>3</b>	<b>ACCOUNT MANAGEMENT STANDARDS.....</b>	<b>2</b>
<b>3.1</b>	<b>Consumer (Beneficiary) Accounts.....</b>	<b>2</b>
3.1.1	Consumer Account Proofing Requirements .....	3
3.1.2	Consumer Account Lifecycle Requirements .....	3
<b>3.2</b>	<b>Professional (Healthcare Industry) Accounts .....</b>	<b>5</b>
3.2.1	Professional Account Proofing Requirements .....	5
3.2.2	Professional Account Lifecycle Requirements .....	6
<b>4</b>	<b>APPROVED .....</b>	<b>7</b>

**(This Page Intentionally Blank)**

## 1 BACKGROUND

Current National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, and Department of Health and Human Services (HHS) *Policy for System Security and Privacy (PS2P)* requirements mandate that all user account passwords expire after 60 days (in accordance with the IA family of controls and HHS-defined parameters). In addition, several other password lifecycle requirements can conflict with best practices and organizational needs when applied to public “consumer” (beneficiary) and public “professional” (provider) user accounts at the Centers for Medicare & Medicaid Services (CMS). NIST- and HHS- required settings are established based on “organizational” users, with “network” access, and undefined “data access” rights. For this reason, NIST and HHS apply conservative password lifecycle requirements.

However, CMS public-facing systems typically have significantly less data-access available to the users that are accessing as a “consumer” of CMS services, or even as a “professional” that is helping to administer those services, and typically expose a smaller portion of the CMS enterprise. The data available is more constrained by utilizing limited data sets, and risk is lowered through specific additional security and privacy mechanisms.

---

## 2 PURPOSE

To address the variety of user types in accordance with NIST and HHS directives, the CMS Chief Information Officer (CIO) may tailor<sup>1</sup> these controls to more-closely align with CMS mission and business objectives, while still maintaining data- and system-protection mechanisms appropriate for the access being granted.

To achieve this objective, Enterprise Information Security Group (EISG) has written this *Risk Management Handbook (RMH)*, Volume III Standard 4.3 to address *Non-Standard Account Authenticator Management* requirements. This standard addresses CMS account concerns focused primarily on the concept of *Beneficiary*, *Provider*, and *Elevated-Provider*<sup>2</sup> user accounts. In order to expand this concept to the entire CMS enterprise, this standard has established their generic user types as *Consumers* and *Professionals*, and developed guidance and requirements appropriate to those general user types.

This standard does not supersede the e-Authentication determination standards and requirements established in *CMS Risk Management Handbook (RMH)*, Volume III, Standard 3.1, *CMS Authentication Standards*. Therefore, systems must adhere to the appropriate e-Authentication levels, as specified in RMH Standard 3.1. If the specific required e-Authentication levels

---

<sup>1</sup> Agencies have some flexibility in applying the minimum baseline security controls in accordance with the guidance provided in Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*. This allows agencies to *tailor* the relevant security control baseline so that it more closely aligns with their mission and business requirements and environments of operation.

<sup>2</sup> Elevated-providers users may have additional rights to create, modify, or delete accounts. In addition, they might be able to reset user account passwords, reactivate disabled accounts, act as proofing “agents” or “proxies”, etc., as permitted by CMS business owner objectives and practices.

established in the RMH Standard 3.1 differ from those discussed below, then those users may not be categorized (or treated) as either *Consumer* or *Professional* users.

---

## 3 ACCOUNT MANAGEMENT STANDARDS

### 3.1 CONSUMER (BENEFICIARY) ACCOUNTS

*Consumer* users typically consist of individual CMS program beneficiaries and/or citizens who wish to access their *own* information and view status, or update basic “profile” information—to include their own *Personally Identifiable Information (PII)*. However, within this population, CMS will also have to account for “*authorized representatives*”<sup>3</sup> (usually family members) who may legally be granted access to those accounts to view or perform designated functions.

Consumer account users fall directly into the E-authentication requirements of Office of Management and Budget (OMB) Memorandum 04-04, *E-Authentication Guidance for Federal Agencies*<sup>4</sup>. Compliance with OMB 04-04 (e-authentication) is required for “*remote*” human (non-organizational<sup>5</sup>) user authentication over “*untrusted data link*”<sup>6</sup> (i.e., the Internet). The required e-authentication level (1 through 4) is contingent on the type, and quantities, of information being accessed, and the risk associated with a breach or disclosure of that data. Typically, for beneficiaries accessing their own data, the e-authentication level is established at level 2<sup>7</sup>. However, accounts where the user is simply “subscribing” to information (e.g., registering their email such that they may receive periodic information or notifications that are not directly tied to their “identity”), might be appropriately established and maintained at e-authentication level 1. No PII or business-related (healthcare administration or commerce) information about an individual may be accessible via an e-authentication level 1 account.

---

<sup>3</sup> Defined at [www.Medicare.gov](http://www.Medicare.gov), FAQ5459, available at <https://questions.medicare.gov/faq.php?id=5007&faqId=5459>. Use CMS form 1696 to get authorized, available at <http://www.cms.gov/Medicare/CMS-Forms/CMS-Forms/CMS-Forms-Items/CMS012207.html>.

<sup>4</sup> OMB Memorandum 04-04, *E-Authentication Guidance for Federal Agencies*, is available at <http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf>. The e-authentication requirements of OMB 04-04 are defined in detail in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63, *Electronic Authentication Guideline*, available at <http://csrc.nist.gov/publications/PubsSPs.html>.

<sup>5</sup> “*Non-organizational users*” are defined in the *CMS Risk Management Handbook (RMH)*, Volume III, Standard 3.1, *CMS Authentication Standards*. *Non-organizational* users include (but are not limited to): *Beneficiaries, Providers, State Medicaid employees and contractors/subcontractors*, and *Non CMS-contracted researchers*.

<sup>6</sup> An *untrusted data link* is defined (in the *CMS Risk Management Handbook (RMH)*, Volume III, Standard 3.1, *CMS Authentication Standards*) as a data-link that cannot be relied upon to enforce CMS security policy and security control requirements. Examples might include (but are not limited to): The Internet, any network not included in a CMS Federal Information Security management Act (FISMA) system, networks included in a CMS FISMA system, but identified as non-compliant with CMS security requirements.

<sup>7</sup> The required e-Authentication level MUST be determined using the appropriate processes associated with RMH Standard 3.1, *CMS Authentication Standards*.

### 3.1.1 CONSUMER ACCOUNT PROOFING REQUIREMENTS

New (or transferred<sup>8</sup>) consumer account users must be proofed, either *in-person* or *remotely*, at the appropriate E-authentication level and using the appropriate minimum NIST proofing standards (*in-person* or *remote*) before establishing a consumer user account.

### 3.1.2 CONSUMER ACCOUNT LIFECYCLE REQUIREMENTS

Beneficiary users accessing via “e-authentication” mechanisms (per OMB 04-04; i.e., non-organizational users, accessing remotely via the Internet), who are only accessing their own data, (or are the authorized representative of up to six [6] designated beneficiary users), may be designated as “consumer accounts”. The following account management standards apply to consumer user accounts:

- User Identification (ID):
  - May be re-used after a minimum of 3 years<sup>9</sup>. However, it may be reused by the same active account within any span.
  - May not be data-linking “keys”.
  - May not be unique PII identifiers.
  - Should be changeable by the user.
  - Should not be system-derived using “guessable” algorithms (unless, upon first use, it is required to be changed.)
- Password re-use:
  - E-authentication level 1 – minimum of 1 generation.
  - E-authentication level 2 – minimum of 6 generations.<sup>10</sup>
  - E-authentication level 3 or 4 – do not qualify as “consumer accounts.”
- Passwords expire:
  - E-authentication level 1 - never.
  - E-authentication level 2 - after 365 days.
  - E-authentication level 3 or 4 – do not qualify as “consumer accounts.”
  - All E-authentication levels - immediately in the event of known or suspected compromise.

---

<sup>8</sup> *Transferred user accounts* are accounts being transferred from one identity/account management system to another. If the user has already been proofed to the minimum NIST standards when enrolled in the previous system, this requirement may be waived.

<sup>9</sup> Per *HHS OCIO Policy for Information Systems Security and Privacy Handbook* and ARS requirement IA-4.

<sup>10</sup> Per ARS requirement IA-5(1).

- Online password recovery requires:
  - Sending a temporary password (or one-time “password reset” link) to a previously-registered (and verified) email address, *or*
  - Online user identity re-validation:
    - E-authentication level 1 – answer at *least* one (1) shared-secret.
    - E-authentication level 2:
      - Answer at least three (3) shared-secrets, *or*
      - Re-proof at e-authentication level 2 (may be performed online).
    - E-authentication level 3 or 4 – do not qualify as “consumer accounts.”
  - Users must change any “system derived” temporary passwords upon first login.
  - Temporary “one-time passwords” or “password reset links” have a limited lifespan of no-more-than 24 hours. Repeat requests automatically “expire” previous (reset links and/or temporary password) requests.
  - User IDs and passwords (including temporary passwords) may never be sent within the same email.
  - Password reset Uniform Resource Locators (URLs) may never contain user identifiers, such as User IDs (e.g., <http://www.passwordreset.cms.gov/JDoe1234/SendMyNewPasswordNow>)
- Online Password Reset:
  - E-authentication level 1 - Passwords may be reset any number of times in a single 24-hour period (however, automated limits should be enforced as a best practice to protect against DoS attacks.).
  - E-authentication level 2 – Passwords may be reset one (1) time in a single 24-hour period (thereafter a Help Desk agent may reset).
  - E-authentication level 3 or 4 – do not qualify as “consumer accounts.”
- Inactive accounts are disabled:
  - E-authentication level 1 – after 24 months of inactivity.
  - E-authentication level 2 – after 180 days of inactivity.
  - E-authentication level 3 or 4 – do not qualify as “consumer accounts.”
- Manual online password change requires first re-*authenticating* (not re-*proofing*) at the appropriate e-authentication level of the applicable account.
- Multiple-function accounts:
  - Consumer accounts cannot be combined with other account types (i.e., must have separate non-consumer accounts), or
  - Account management parameters default to those settings required for the most restrictive access applicable to the user.
- All remaining *Acceptable Risk Safeguards (ARS)* requirements pertaining to user account management apply.

## 3.2 PROFESSIONAL (HEALTHCARE INDUSTRY) ACCOUNTS

For professional users, including healthcare providers and other healthcare industry professional users<sup>11</sup> (non-organizational<sup>12</sup>) accessing via “e-authentication” mechanisms (per OMB M-04-04), we can designate as *Professional* accounts, within the below listed constraints.

Professional account users also fall into the e-Authentication requirements of OMB Memorandum 04-04. Compliance with OMB M-04-04 (e-authentication) is required for “remote” human (*non-organizational*) user authentication over “untrusted data link” (i.e., the Internet). The required authentication level (1 through 4) is contingent on the type, and quantities, of information being accessed, and the risk associated with a breach or disclosure of such data.

Accounts where the Professional user is simply “subscribing” to information (e.g., registering their email such that they may receive periodic information or notifications that are not directly tied to their “identity”), may be established and maintained at e-authentication level 1. No PII, or (non-public) business-related (healthcare administration or commerce) information about an individual or commercial enterprise, may be accessible via an e-authentication level 1 account.

Accounts where a Professional user can only submit, review, and/or update sensitive information that *they* have provided *during the current session*, may be established and maintained at e-authentication Level 2, provided that the applicable data is no longer accessible in subsequent sessions, and the only data available via subsequent sessions is appropriate for e-authentication level 2.

Typically, Professionals, in the due course of performing their employment functions, are accessing data that includes PII/Protected Health Information (PHI) for individuals, other than themselves, for the purposes of conducting “healthcare administration” or “healthcare commerce”. These accounts will typically require e-authentication level 3 (or in some cases Level 4.)

### 3.2.1 PROFESSIONAL ACCOUNT PROOFING REQUIREMENTS

New (or transferred<sup>13</sup>) professional account users must be proofed, either *in-person* or *remotely*, at the appropriate E-authentication level and using the appropriate minimum NIST proofing standards (*in-person*<sup>14</sup> or *remote*) before establishing a professional user account.

---

<sup>11</sup> *User* accounts do NOT include accounts with “elevated privileges” such as group administrators with the ability to *create, delete, or reset other* user accounts.

<sup>12</sup> Organizational users and non-organizational users are defined in the CMS *Risk Management Handbook (RMH)*, Volume III, Standard 3.1, *CMS Authentication Standards*.

<sup>13</sup> *Transferred user accounts* are accounts being transferred from one identity/account management system to another. If the user has already been proofed to the minimum NIST standards when enrolled in the previous system, this requirement may be waived.

<sup>14</sup> In the case of *local* proofing, CMS may also accept the local proofing standards established by the *Immigration Reform and Control Act of 1996 (IRCA)*, using the applicable *Employment Eligibility Verification Form I-9*.

### 3.2.2 PROFESSIONAL ACCOUNT LIFECYCLE REQUIREMENTS

The following account management standards apply to Professional user accounts:

- New users must be proofed at the appropriate E-authentication level before establishing a professional account.
- User ID:
  - May be re-used after a minimum of 3 years<sup>15</sup>. However, it may be reused by the same active account within any span.
  - May not be data-linking “keys”.
  - May not be unique PII identifiers.
  - Should be changeable by the user.
  - Should not be system-derived using “guessable” algorithms (unless, upon first use, it is required to be changed.)
- Password re-use:
  - E-authentication level 1 – minimum of 1 generation.
  - E-authentication level 2 through 4 – minimum of 6 generations<sup>16</sup>.
- Passwords expire:
  - E-authentication level 1 - never.
  - E-authentication level 2 and 3 - after 180 days.
  - E-authentication level 4 - after 60 days.
  - All Levels - immediately in the event of known or suspected compromise.
- Online password recovery requires:
  - Sending a temporary password (or one-time “password reset” link) to a previously-registered (and verified) email address, *or*
  - Online user identity re-validation:
    - E-authentication level 1 – answer at least one (1) shared-secret.
    - E-authentication level 2:
      - Answer at least three (3) shared-secrets, *or*
      - Re-proof at e-authentication level 2 (may be performed online).
    - E-authentication level 3 – Re-proof at e-authentication level 3 (may be performed online).
    - E-authentication level 4 – may not be performed online.
  - Users must change any “system derived” temporary passwords upon first login.
  - Temporary “one-time passwords” or “password reset links” have a limited lifespan of no-more-than 12 hours. Repeat requests automatically “expire” previous requests.

---

<sup>15</sup> Per *HHS OCIO Policy for Information Systems Security and Privacy Handbook* and ARS requirement IA-4.

<sup>16</sup> Per ARS requirement IA-5(1).

- User IDs and passwords (including temporary passwords) may never be sent within the same email.
- Password reset URLs may never contain user identifiers, such as User IDs (e.g., <http://www.passwordreset.cms.gov/JDoe1234/SendMyNewPasswordNow>)
- Online Password Reset:
  - E-authentication level 1 - Passwords may be reset any number of times in a single 24-hour period (however, automated limits should be enforced as a best practice to protect against DoS attacks.).
  - E-authentication level 2 through 4 – Passwords may be reset one (1) time in a single 24-hour period (thereafter a Help Desk agent may reset).
- Inactive accounts are disabled:
  - E-authentication level 1 – after 24 months of inactivity.
  - E-authentication level 2 through 3 – after 180 days of inactivity.
- Manual online password change requires first re-*authenticating* (not re-*proofing*) at the appropriate e-authentication level of the applicable account.
- Multiple-function accounts:
  - Professional accounts cannot be combined with other account types (i.e., must have separate non-Professional accounts), or
  - “Account management parameters” default to those settings required for the “most restrictive access” applicable to the user.
- All remaining ARS pertaining to user account management requirements apply.

---

## 4 APPROVED

/s/ 10/30/2013

Tony Trenkle  
CMS Chief Information Officer and  
Director, CMS Office of Information Services

*This document will be reviewed periodically, but no less than annually, by the Enterprise Information Security Group (EISG), and updated as necessary to reflect changes in policy or process. If you have any questions regarding the accuracy, completeness, or content of this document, please contact the EISG at <mailto:ciso@cms.gov>.*

**(This Page Intentionally Blank)**