PassGeni

# COMPLIANCE CHEAT SHEET SERIES

Six reference documents for security and compliance teams.

**01** HIPAA + PCI-DSS Password Requirements
**02** SOC 2 + ISO 27001 Password Requirements
**03** NIST SP 800-63B Plain-English Guide
**04** DoD + Federal Government Password Requirements
**05** Password Security for Healthcare Teams
**06** Password Policy Template (HIPAA-Ready)

All documents free — no account required — passgeni.ai

*This series is a reference guide. Verify requirements against current official standards.*

VOL. 01

# HIPAA + PCI-DSS Password Requirements

Quick reference for compliance teams

## HIPAA Password Requirements

45 CFR § 164.308(a)(5)(ii)(D) · HHS.gov · NIST SP 800-66 Rev. 2 (2023)

| Requirement | HIPAA Standard | PassGeni |
|---|---|---|
| Minimum length | 8 characters (12 recommended by HHS) | Slider → 12 |
| Uppercase letters | Required in complexity policy | Uppercase ON |
| Lowercase letters | Required | Lowercase ON |
| Numbers | Required | Numbers ON |
| Special symbols | Required | Symbols ON |
| No dictionary words | Must resist dictionary attack | AI seeding enforced |
| No username in password | Required | Client-side check |
| Password history | Last 6 passwords cannot be reused | History panel |
| Maximum age | 90 days (recommended) | Rotation reminder |
| Account lockout | After 5 failed attempts | Outside generator scope |
| Multi-factor auth | Strongly recommended | Outside generator scope |

**PassGeni HIPAA Preset — One click, all 7 password-level requirements auto-configured.**
Compliance reference: HHS.gov · 45 CFR Part 164 · NIST SP 800-66 Rev. 2 (2023)

## PCI-DSS v4.0 Password Requirements

Requirement 8.3 — Identify Users · Requirement 8.6 — Manage System/App Accounts

| Requirement | PCI-DSS v4.0 Standard | PassGeni |
|---|---|---|
| Minimum length | 12 characters (up from 7 in v3.2.1) | Slider → 12 |
| Complexity | Upper + lower + number + symbol | All options ON |
| No dictionary words | Must resist guessing attacks | AI seeding enforced |

| Requirement | PCI-DSS v4.0 Standard | PassGeni |
|---|---|---|
| No username in password | Required | Client-side check |
| Password history | Last 4 passwords cannot be reused | History panel |
| Maximum age | 90 days for non-MFA accounts | Rotation reminder |
| Change on first use | Required for new or reset passwords | Outside generator scope |
| Account lockout | After 10 failed attempts | Outside generator scope |
| Multi-factor auth | Required for all admin access | Outside generator scope |
| Shared accounts | Must not use shared/generic passwords | Bulk generator available |

**PassGeni PCI-DSS Preset — One click, all 8 password-level requirements auto-configured.**
Reference: PCI Security Standards Council · PCI-DSS v4.0 — March 2022 · Full compliance: March 2025

⬡ NIST SP 800-63B aligned · ◈ Zero storage · ✦ Client-side only · ◎ No account needed

VOL. 02

# SOC 2 + ISO 27001 Password Requirements

Quick reference for compliance teams

## SOC 2 Password Requirements

Trust Services Criteria — CC6.1, CC6.2, CC6.3 · AICPA TSC 2017 (updated 2022)

| Requirement | SOC 2 Criteria | PassGeni |
|---|---|---|
| Minimum length | Not specified — auditor expects 12+ | Slider → 12 |
| Complexity | Must 'restrict access' — complexity required | All options ON |
| Unique per system | Required — no password reuse across systems | Generate per-account |
| No shared credentials | CC6.2 — individual accountability required | Bulk per-user |
| Password history | Expected — typically last 10 | History panel |
| Maximum age | Expected — typically 90 days | Rotation reminder |
| Privileged accounts | Stronger controls required (16+ chars) | Slider → 16+ |
| Service accounts | Must be documented and rotated | Bulk generator + export |
| Multi-factor auth | Strongly expected by auditors | Outside generator scope |

**What SOC 2 auditors actually check:**

— Written password policy document — Proof policy is technically enforced

— Access logs for privileged accounts — Evidence of regular rotation

PassGeni compliance preset satisfies the technical enforcement evidence requirement.

Important: SOC 2 has no fixed password standard. Auditors apply professional judgment. Your auditor may require more.

## ISO 27001:2022 Password Requirements

Annex A — Control 5.17 · Authentication information

| Requirement | ISO 27001:2022 Control 5.17 | PassGeni |
|---|---|---|
| Minimum length | Not fixed — 'sufficiently long' (12+ expected) | Slider → 12 |
| Quality | Must be 'of sufficient quality' — complexity implied | All options ON |
| No dictionary words | Must resist common attack methods | AI seeding enforced |

| Requirement | ISO 27001:2022 Control 5.17 | PassGeni |
|---|---|---|
| Confidentiality | Must not be shared or written in plain text | Zero storage by design |
| Uniqueness | Different password for each system | Generate per-account |
| No default passwords | Must change all default credentials | Outside generator scope |
| Password history | Required — no reuse of recent passwords | History panel |
| Maximum age | Required — typical implementation is 90 days | Rotation reminder |
| Privileged access | PAM controls — stronger passwords required | **Slider → 16+, Post-Quantum** |

**ISO 27001 vs ISO 27002 — ISO 27001 sets the requirement. ISO 27002 provides implementation guidance.**
ISO 27002:2022 §5.17 recommends: min 12 characters, mixed classes, no personal info, no sequential patterns.
PassGeni ISO 27001 preset implements all ISO 27002 §5.17 technical recommendations.

## Where SOC 2 and ISO 27001 Agree

- Formal written password policy
- Technical enforcement of that policy
- Evidence of compliance for audit
- Stronger controls for privileged access
- Regular rotation and history enforcement
- No shared or generic accounts

Reference: AICPA TSC 2017 · ISO/IEC 27001:2022 · ISO/IEC 27002:2022

VOL. 03

# NIST SP 800-63B The Password Standard That Changes Everything

Plain-English breakdown for security and compliance teams

## What NIST SP 800-63B Actually Is

NIST Special Publication 800-63B is the US federal standard for digital identity authentication. Published in 2017, revised continuously. It is the most cited password standard in the world — referenced by HIPAA auditors, PCI-DSS, SOC 2 examiners, and security engineers globally.

Most security teams have heard of it. Almost nobody has read all 79 pages. This guide is the 79 pages in plain English.

## The Five Rules NIST Changed Forever

### Rule 1 — Passphrases beat complex passwords

**Old thinking: "P@ssw0rd1!" is strong because it has upper, lower, numbers, and symbols.**

NIST 800-63B §5.1.1.2: It is not strong. Attackers know every common substitution pattern.

"correct-horse-battery-staple" — four random words — is cryptographically stronger and memorisable.

Recommendation: Min 8 chars. Recommend 15+. Allow all Unicode. Support passphrases. Do not require complexity rules.

PassGeni: Passphrase tab → NIST 800-63B mode. Four random words from profession vocabulary. 50+ bits of entropy.

### Rule 2 — Mandatory rotation is harmful

**Old thinking: Change your password every 90 days.**

NIST 800-63B §10.2.1: "Verifiers SHOULD NOT require memorised secrets to be changed arbitrarily."

Why: Forced rotation causes predictable patterns (Spring2024! → Summer2024!). Users degrade password quality.

Exception: Change ONLY when there is evidence of compromise — not on a calendar schedule.

PassGeni: Rotation reminders (Team plan) are event-triggered, not calendar-based.

### Rule 3 — Check against known breached passwords

**NIST 800-63B §5.1.1.2: Verifiers SHALL compare passwords against a list of known compromised values.**

This includes: passwords from breach corpora, dictionary words, repetitive patterns, context-specific words.

PassGeni Breach Checker: k-anonymity via HaveIBeenPwned. Your password never leaves your device.

### Rule 4 — Composition rules are counterproductive

**Old thinking: Must contain uppercase, lowercase, number, symbol.**

NIST 800-63B §5.1.1.2: "Verifiers SHOULD NOT impose other composition rules."

Why: Composition rules reduce password space by making passwords predictable. Users satisfy minimally: "Password1!"

Correct approach: Minimum length (15+) + breach checking. Length alone beats complexity.

PassGeni: Complexity options available but not forced. Passphrase mode for NIST-pure compliance.

### Rule 5 — Security questions are prohibited

**NIST 800-63B §5.1.1.2: "Verifiers SHOULD NOT use knowledge-based authentication (KBA) or security questions."**

Why: Your mother's maiden name is findable on LinkedIn in under 10 minutes. KBA provides false confidence.

If your system still uses security questions, you are out of NIST 800-63B alignment.

## NIST 800-63B Quick Reference

| What NIST Says | What It Means | PassGeni Setting |
|---|---|---|
| Min 8 chars, recommend 15+ | Length beats complexity | Slider → 15+ |
| Support passphrases | 4 random words is valid and strong | Passphrase tab |
| No mandatory rotation | Only rotate on compromise | Event-based reminders |
| Check breach lists | Every new password | Breach Checker tool |
| No composition rules required | Don't force symbols | Optional, not forced |
| No security questions | Remove KBA from systems | Outside generator scope |
| Allow all Unicode | Including foreign scripts | 12 language scripts |
| Do not truncate passwords | Don't cut passwords short | Up to 32 characters |

## NIST 800-63B Assurance Levels

| Level | Name | Requirements | Suitable For |
|---|---|---|---|
| AAL1 | Basic | Password alone. Min 8 chars. Breach check. | Low-risk applications |
| AAL2 | Enhanced | Password + second factor. Phishing-resistant MFA preferred. | Healthcare, financial, personal data |
| AAL3 | High | Hardware cryptographic authenticator. Physical possession factor. | Government, critical infrastructure |

Most enterprise applications require AAL2. PassGeni addresses the password component of AAL1 and AAL2.

Reference: NIST SP 800-63B Digital Identity Guidelines — Authentication & Lifecycle Management

VOL. 04

# DoD + Federal Government Password Requirements

For government contractors and federal IT teams

## DoD Password Requirements

DoD Instruction 8520.03 · DISA STIG — Application Security · CMMC 2.0 Level 2

| Requirement | DoD / DISA Standard | PassGeni |
|---|---|---|
| Minimum length | 15 characters | Slider → 15 |
| Uppercase letters | Required | Uppercase ON |
| Lowercase letters | Required | Lowercase ON |
| Numbers | Required | Numbers ON |
| Special symbols | Required — at least 2 | Symbols ON |
| No dictionary words | Required | AI seeding enforced |
| Password history | Last 10 passwords prohibited | History panel |
| Maximum age | 60 days (all accounts) | Rotation reminder |
| Minimum age | 1 day (prevent immediate reuse) | Outside generator scope |
| Account lockout | After 3 failed attempts | Outside generator scope |
| Multi-factor auth | Required for all CUI-level access | Outside generator scope |
| Post-Quantum readiness | Recommended — NSA CNSA 2.0 | Post-Quantum mode |

**CMMC 2.0 Level 2 — Password Specific:**

Practice IA.L2-3.5.7: "Enforce a minimum password complexity and change of characters when new passwords are created."

PassGeni DoD preset → 15 chars minimum, all complexity classes, Post-Quantum mode. Satisfies IA.L2-3.5.7.

## Federal / FedRAMP Password Requirements

NIST SP 800-53 Rev. 5 — IA-5 · FedRAMP Moderate Baseline · FISMA Compliance

| Requirement | NIST 800-53 IA-5 | PassGeni |
|---|---|---|
| Minimum length | 12 chars (15 for privileged) | Slider → 15 |
| Complexity | Mixed case + numbers + symbols | All options ON |

| Requirement | NIST 800-53 IA-5 | PassGeni |
|---|---|---|
| No reuse | Last 24 passwords (high impact) | History panel |
| Maximum age — privileged | 60 days | Rotation reminder |
| Maximum age — standard | 90 days | Rotation reminder |
| Temporary passwords | Must change on first use | Outside generator scope |
| Automated enforcement | Technical controls must enforce policy | **PassGeni preset = evidence** |
| Privileged accounts | Separate credentials from standard | Bulk generator — separate |

**NIST 800-53 IA-5(1) — Password-Based Authentication:**

"Enforce minimum password complexity and length... Prohibit the same password as used in previous [n] passwords..."

FedRAMP Moderate requires IA-5(1). FedRAMP High requires IA-5(1) + IA-5(4).

## NSA CNSA 2.0 — Post-Quantum Readiness

NSA issued CNSA 2.0 in 2022, mandating post-quantum cryptographic algorithms for national security systems by 2033. For passwords:

- Minimum 128-bit classical security
- Resistant to Grover's algorithm
- Extended length — 20+ characters recommended
- Avoid patterns vulnerable to quantum search

**PassGeni Post-Quantum Mode: 20+ character minimum, extended character pool, pattern avoidance, NIST PQC 2024 aligned.**

Recommended for any contractor handling classified or sensitive government information.

Reference: DoD Instruction 8520.03 · DISA STIG · CMMC 2.0 · NIST SP 800-53 Rev.5 · NSA CNSA 2.0

VOL. 05

# Password Security for Healthcare Teams

For clinicians, administrators, and IT — no jargon

## Why Healthcare Passwords Matter More

Healthcare is the most breached industry on the planet — for the ninth consecutive year in 2024. (IBM Cost of a Data Breach Report)

| Metric | Data |
|---|---|
| Average cost of a healthcare breach | $10.9 million |
| Average cost — all other industries | $4.5 million |
| Top attack vector: stolen or weak credentials | 61% of breaches |
| Top attack vector: phishing → credential theft | 49% of breaches |
| Top attack vector: insider threats | 35% of breaches |

A strong password policy, consistently applied, directly addresses the #1 attack vector.

## The Systems Your Team Logs Into Every Day

### EHR / EMR Systems (Epic, Cerner, athenahealth)

Stores: complete patient records, diagnoses, medications, treatment history. Breach impact: PHI exposure, HIPAA violation, patient harm.

| Setting | Requirement |
|---|---|
| Minimum length | 15 characters |
| Character types | Upper + lower + number + symbol |
| Rotation | Every 90 days |
| History | Never reuse last 6 passwords |
| MFA | Required on all remote access |

### Practice Management Software (Kareo, Drchrono, Meditech)

HIPAA applies to billing systems equally. A breach of scheduling data is a HIPAA breach. Apply the same requirements as your EHR.

### Medical Imaging / PACS (Sectra, Agfa, GE)

X-rays, MRIs, and CT scans are PHI. Shared logins are a HIPAA violation regardless of team trust level.

### Communication Tools (Teams, Slack, Halo Health)

If patient names appear in context, HIPAA applies. Never discuss identifiable patient information in consumer messaging apps.

## The HIPAA Audit Checklist

| Auditor Requirement | How to Satisfy It |
|---|---|
| Written password policy document | PassGeni Policy Generator (Team plan) |
| Evidence of technical enforcement | **PassGeni preset = documented technical enforcement** |
| Individual accountability | No shared logins — each user has own credentials |
| Evidence of rotation enforcement | System logs or rotation reminder records |
| BAA with PassGeni required? | No — PassGeni stores zero PHI. Client-side only. |

## The Three Mistakes Healthcare Teams Make Most Often

### Mistake 1 — Shared login credentials

> **"We all use the same login for the lab system because it's faster."**
>
> HIPAA §164.312(a)(2)(i) requires unique user identification. Shared credentials make individual accountability impossible.
>
> If there is a breach, you cannot prove who accessed what. That is the violation.
>
> Fix: Use PassGeni Bulk Generator to create unique strong passwords for each team member in seconds.

### Mistake 2 — Writing passwords on paper or in notes apps

> **A sticky note under the keyboard. A "Passwords" folder in iPhone Notes. A Word document called logins.docx.**
>
> Physical theft → instant access. iCloud sync → unencrypted cloud storage. No audit trail if compromised.
>
> Fix: PassGeni generates passwords that are strong AND profession-contextually memorable.

### Mistake 3 — Same password across systems

> **A breach of any one system compromises all. Credential stuffing attacks test stolen passwords across hundreds of systems automatically.**
>
> Fix: One unique password per system. PassGeni generates a new strong password for each account in under 3 seconds.

## What to Set in PassGeni for Healthcare

| System | Length | Mode | Rotation |
|---|---|---|---|
| EHR (Epic, Cerner) | 15 | HIPAA preset | 90 days |
| Practice Management | 12 | HIPAA preset | 90 days |
| Medical Imaging (PACS) | 15 | HIPAA preset | 90 days |

| System | Length | Mode | Rotation |
|---|---|---|---|
| Admin email | 15 | Passphrase | 90 days |
| Patient portal admin | 15 | HIPAA preset | 90 days |
| Wi-Fi / network | 20 | Post-Quantum | 1 year |
| VPN | 20 | Post-Quantum | 90 days |

Reference: 45 CFR Part 164 · HHS.gov · NIST SP 800-66 Rev.2

*This guide is educational reference, not legal advice.*

VOL. 06

# Password Policy Template

HIPAA · PCI-DSS · SOC 2 Aligned — Customise with your organisation details

## Document Header

| Field | Value |
|---|---|
| Organisation Name | |
| Policy Owner | |
| Effective Date | |
| Review Date | |
| Version | |
| Approved By | |

## 1. Purpose

This policy establishes requirements for the creation, maintenance, and protection of passwords used to access [ORGANISATION NAME] information systems, networks, and data.

This policy applies to all employees, contractors, vendors, and third parties who access [ORGANISATION NAME] systems. Designed to comply with:

- HIPAA Security Rule — 45 CFR §164.308(a)(5)(ii)(D)
- PCI-DSS v4.0 — Requirements 8.3 and 8.6
- NIST SP 800-63B — Memorised Secret Authentication
- [Add applicable standard: SOC 2 / ISO 27001 / DoD STIG]

## 2. Scope

This policy applies to all information systems owned or managed by [ORGANISATION NAME], and all user accounts including: standard user, administrative and privileged, service and system, and temporary and contractor accounts.

## 3. Password Requirements

### 3.1 Standard User Accounts

| Parameter | Requirement |
|---|---|
| Minimum length | 15 characters |
| Uppercase letters | At least 1 required (A–Z) |
| Lowercase letters | At least 1 required (a–z) |
| Numbers | At least 1 required (0–9) |

| Parameter | Requirement |
|---|---|
| Special characters | At least 1 required (!@#$%^&*) |
| Dictionary words | Prohibited |
| Sequential patterns | Prohibited (12345, abcde, qwerty) |
| Username in password | Prohibited |
| Password history | Last 10 cannot be reused |
| Maximum age | 90 days |
| Minimum age | 1 day |

### 3.2 Privileged and Administrative Accounts

| Parameter | Requirement |
|---|---|
| Minimum length | 20 characters |
| Character requirements | Same as 3.1 — stricter enforcement |
| Password history | Last 24 cannot be reused |
| Maximum age | 60 days |
| Multi-factor authentication | REQUIRED — no exceptions |

### 3.3 Service and System Accounts

| Parameter | Requirement |
|---|---|
| Minimum length | 20 characters |
| Maximum age | 90 days or per system change event |
| Human access | Must not be used by human users |
| Documentation | Must be documented in asset register |

## 4. Password Creation

### 4.1 Approved Methods

- PassGeni (passgeni.ai) — HIPAA/PCI-DSS preset
- Approved password manager random generator
- Manual creation meeting all requirements in Section 3.1

### 4.2 Prohibited Patterns

- First name, last name, or username
- Organisation name or abbreviation
- Birthdate, anniversary, or memorable date
- Sequential keyboard patterns (qwerty, asdf, 1234)
- Single word with simple substitution (P@ssw0rd)

— Passwords found in known breach datasets

### 4.3 Breach Checking

Before adopting a new password, verify it has not appeared in known data breaches using PassGeni's Breach Checker tool. The full password never leaves the device (k-anonymity protocol).

### 4.4 Passphrases

Four or more random words are an approved and recommended alternative to complex passwords, consistent with NIST SP 800-63B. Use PassGeni's Passphrase mode.

## 5. Password Protection

Passwords must not be shared with any person, written on paper or stored in unencrypted documents, or communicated via email, SMS, or chat in plain text.

If a password must be shared (emergency access): use PassGeni Secure Share for one-time encrypted link delivery; change the password immediately after; document the event in the IT access log.

If suspected to be compromised: change it immediately; report to IT Security within 1 hour; do not wait for confirmation.

## 6. Compliance and Enforcement

6.1 Monitoring — IT systems enforce password requirements technically. Non-compliant passwords are rejected by the system.

6.2 Violations — May result in temporary suspension, disciplinary action, or regulatory notification if a breach results.

6.3 Exceptions — Require written request, business justification, approval by [CISO / IT Director], and a time-limited review date.

6.4 Review — Annually, or following a security incident, material regulatory change, or significant technology change.

## 7. Definitions

| Term | Definition |
|---|---|
| Credential | A username and associated authentication factor (password, token, certificate) |
| PHI | Protected Health Information — any individually identifiable health information under HIPAA |
| Privileged Account | Account with administrative, root, or elevated access to systems or data |
| Service Account | A non-human account used by applications, scripts, or automated processes |
| Passphrase | Four or more random words providing high entropy and memorability. NIST 800-63B approved. |
| Breach Dataset | Published collection of compromised credentials from known security incidents |
| MFA | Multi-Factor Authentication — requires two or more independent verification factors |

## Policy Approval

| Role | Name | Signature | Date |
|---|---|---|---|
| Prepared by | | | |
| Title | | | |
| Approved by | | | |
| Title | | | |
| Next review date | | | |

*This template is provided for reference. Have your legal or compliance counsel review before adoption.*

PassGeni · passgeni.ai · hello@passgeni.ai · 2025