PointClickCare®

Implication for: SNF, SL

July 2, 2025

Regulatory Briefing

PointClickCare will enforce multi-factor authentication (MFA) for remote system access starting August 1, 2025, to enhance patient data security and align with industry best practices, such as NIST Cyber Security Framework and NIST 800-53, revision 5, moderate baseline controls. MFA is a widely adopted practice to protect sensitive data such as Protected Health Information (PHI), Personally Identifiable Information (PII), and other sensitive information. MFA is also consistent with the proposed changes in the HIPAA Security Rule, under consideration by HHS.

Enforcement of Multi-Factor Authentication (MFA) Impact on Surveyor Access

Starting on Aug 1, 2025, PointClickCare will begin enforcing multi-factor authentication (MFA) for system access to protect patient data and comply with the following federal regulations:

- **HIPAA Security Rule (45 CFR §164.312)**:
  - **§164.312(a)(1)**: Requires "unique user identification" and verification of ePHI access—interpreted by HHS as necessitating strong authentication (e.g., MFA).
  - **§164.312(d)**: Mandates verifying user identity, with HHS/OCR citing MFA as a best practice.
- **NIST SP 800-63-3** (Adopted by HHS): Requires MFA for remote access to high-risk systems (like ePHI).
- **HHS Security Risk Assessment**: Designates MFA as critical for mitigating unauthorized access risks.

Surveyors may face challenges enabling MFA in certain jurisdictions and on certain devices. In these instances, facilities may use these approved options to provide surveyor access while still maintaining compliance with the above regulations:

1. Using a Pre-Configured Trusted Facility Laptop

- **Pre-configured facility laptops** ensure seamless MFA without external dependencies.
- Aligns with internal policies and reduces access barriers.

2. Using a Trusted Network Address

- If pre-configured facility laptops are unavailable, surveyors may use the public IP address of the facility as a trusted (compliant) network connection.
  - In this scenario, the surveyor is assigned an IP address by the facility
  - The public IP address to the surveyor must be static and configured in the PCC Administration interface by an authorized PCC Facility Administrator.

- This may require the use of a facility **VPN.**
- Maintains compliance with PointClickCare authentication requirements.
- If surveyors are already using VPNs assigned by their employer and not the facility, then the public IP address/range of the surveyor VPN would need to be configured in the PCC Administration interface by authorized PCC Facility Administrator.

3. Configuring Surveyors for PCC MFA

- In this scenario, the PCC facility administrator must configure the Surveyor as a remote worker in the PCC Administration interface.
- The surveyor must then install and activate SMS or TOTP based Authenticator applications such as Google/Microsoft Authenticator on Surveyor phones.

As a courtesy we suggest that you communicate these changes and options with your state surveyors prior to your next survey, ensuring that they are informed prior to entering your facility.

If you still have questions? Contact your Customer Success Manager (CSM) or contact us at support@pointclickcare.com

HIPAA Security Rule Notice of Proposed Rulemaking to Strengthen Cybersecurity for Electronic Protected Health Information |