DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop S2-26-12
Baltimore, Maryland 21244-1850

DATE: January 17, 2025

FROM: Brent Weaver
Director, Data and Systems Group (DSG)
Center for Medicaid and CHIP Services (CMCS)
Centers for Medicare & Medicaid Services (CMS)

Patrick Newbold
Director, Office of Information Technology (OIT) &
CMS Chief Information Officer (CIO)
Centers for Medicare & Medicaid Services (CMS)

SUBJECT: Cyber Security for State Medicaid Programs

Center for Medicaid & CHIP Services (CMCS) is issuing a reminder to emphasize the importance for Medicaid and CHIP agencies, their contractors, and vendors to safeguard Protected Health Information (PHI) and Personal Identifiable Information (PII), and maintain business operations during natural or man-made disasters, **including cyberattacks**.

Recent Cybersecurity Trends

The Department of Health and Human Services (HHS) Office for Civil Rights (OCR) reports a substantial increase in reports of large breach reports received over the last five years. From 2018-2023, reports of large breaches increased by 102%, and the number of individuals affected by such breaches increased by 1,002%, primarily because of increases in hacking and ransomware attacks. In 2023, over 167 million individuals were affected by large breaches. Since 2019, large breaches caused by hacking and ransomware have increased 89% and 102%, respectively."[1] The Change Healthcare cyberattack exemplifies the profound disruption such events can cause.

Organizations' Obligations to Protect PHI

Federal laws and regulations mandate the protection of PHI. Key requirements include, but are not limited to:

[1] https://www.hhs.gov/hipaa/for-professionals/security/hipaa-security-rule-nprm/index.html

- Compliance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules, which mandate the confidentiality, integrity, and availability of PHI
- Compliance with the National Institute of Standards and Technology (NIST) Cybersecurity Framework or a similar framework that can be mapped back to NIST standards
- Implementation of Multi-Factor Authentication (MFA) for all systems and environments to protect sensitive data and prevent unauthorized access
- Encryption of stored or transmitted data in all environments
- Conducting an annual risk analysis to ensure effective security and privacy safeguards are implemented is strongly recommended
- Strengthening requirements for planning for contingencies and responding to security incidents or cybersecurity attacks
- Adherence to Medicaid regulations and other applicable requirements, ensuring robust privacy safeguards
- Compliance of all first-tier, downstream, and related entities (FDRs), including contracted vendors, to ensure their operations align with contractual obligations

Failure to meet these requirements may result in compliance or enforcement actions by CMCS. Medicaid and CHIP programs should rigorously oversee vendor activities to mitigate risks associated with cyber threats.

Maintaining Business Operations

Medicaid and CHIP programs should ensure uninterrupted operations, including enrollment, claims processing, and timely payment to providers. To ensure uninterrupted business operations, Medicaid and CHIP agencies' business continuity plans should:

- Perform risk analysis on an annual basis to determine the priority of restoration of the information systems and technology assets
- Address IT system restoration and ongoing operations following a disruption
- Include contingency measures, such as backup vendors, to sustain critical functions
- Incorporate MFA as a key security measure across all access points to critical systems and data

While flexibilities may be granted during declared emergencies, CMS expects organizations to maintain compliance during other disruptions, including cyberattacks. CMS encourages states to engage CMS for technical assistance to help the state ensure they remain in compliance.

Requirements

Medicaid and CHIP Agencies are subject to Federal regulations at 42 CFR Part 431 Subpart F, Safeguarding Information on Applicants and Beneficiaries, and the Administrative Simplification provisions under the Health Insurance Portability and Accountability Act (HIPAA) requirements as specified in 45 CFR Part 160 and Part 164. Further, States are bound by the requirements in section 1902(a)(7) of the Social Security Act, which require states to

provide safeguards that restrict the use or disclosure of information concerning applicants and beneficiaries for purposes directly connected with the administration of the Medicaid program.

The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA-covered entities and their business associates to provide notification following a breach of unsecured protected health information. Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC), apply to vendors of personal health records and their third-party service providers, pursuant to section 13407 of the HITECH Act.

Recommended Practices

CMS encourages adherence to the HHS Cyber Performance Goals and the President's National Security Memorandum-22, which promote cyber resilience and critical infrastructure security. Some key recommendations include:

- Implementing MFA for all users, including internal staff and external vendors, as a foundational cybersecurity practice.
- Striving to meet "essential" cyber goals within 12 months and "enhanced" goals within two years.
- Implementing strong encryption of data at rest and in transit to prevent PHI from being compromised.
- Ensuring software and hardware is updated and patched regularly basis
- Routinely performing penetration testing on systems and swiftly remediating any issues that are discovered.
- Identifying single points of failure in payment and claims processing systems to reduce vulnerabilities.
- Performing system and data backups and testing data restoration on a regular cadence.
- Properly training staff on their role and expectations in preventing cybersecurity attacks.

Conclusion

Medicaid and CHIP agencies are encouraged to take proactive steps to safeguard PHI and ensure operational continuity. Cyber resilience is a shared responsibility extending to all contractors and vendors; robust collaboration is needed between all stakeholders to improve our security posture and prevent future cyberattacks. By adopting best practices, Medicaid and CHIP agencies can better protect the interests of their members and maintain compliance with Federal requirements. Additional resources and Cyber Security Guidance Material are available via HHS.gov at **https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html**

Should states have questions about this information or need technical assistance regarding this topic, please contact Brent Weaver, brent.weaver@cms.hhs.gov.