

# Password Security Best Practices for Chiropractic Practices

In the current healthcare technology landscape — which includes robotics, telehealth, artificial intelligence, 3D printing, nanomedicine, virtual reality, and more — password security might seem archaic. Chiropractors have used passwords for years to log in to various organizational systems, and doing so has likely become second nature. Recently, however, cyberattacks and data breaches have heightened security concerns for chiropractic practices, emphasizing the need to develop new security strategies and revisit old protocols.

Although the concept and purpose of passwords are not new, these security controls still prove troublesome in chiropractic care, where “deficient user authentication and excessive user permissions are frequently named as the leading risks to the enterprise.”<sup>1</sup> Examples of common password issues include staff creating weak passwords, sharing passwords, writing passwords on paper, posting passwords in visible locations, and forgetting to log out of systems.

Unfortunately, even minor oversights in password security can result in significant consequences. Failure to follow best practices for creating, updating, and recovering passwords might put confidential and protected information at risk, potentially increasing the risk of cyberattacks, data breaches, and HIPAA violations.

Below are lists of “do’s” and “don’ts” for password security, curated from various cybersecurity resources.<sup>2</sup> Use these recommendations to review your chiropractic practice’s current password protocols and pinpoint potential security issues. Proactively addressing security gaps can help mitigate cybersecurity risks and protect sensitive and proprietary information.

## Password Do's

- Require a password login for all organizational systems that contain protected health information, confidential files, or sensitive data.
- Change default passwords that come with systems or programs immediately after installation.
- Establish security standards that require passwords to be at least eight characters long and use a combination of uppercase and lowercase letters, numbers, and symbols. Some organizations, such as the Cybersecurity and Infrastructure Security Agency, recommend a minimum of 16 characters.
- Consider requiring passphrases rather than passwords for systems or programs that contain highly sensitive information. A passphrase is typically a sentence or a combination of words, numbers, and symbols. Passphrases typically are longer than passwords.
- Encourage staff members to break common password weaknesses, such as placing capital letters at the beginning of a password and numerals at the end.
- Use two-factor or multi-factor authentication. This method involves a password and at least one other identifying technique, such as an electronic identification card, key fob, or fingerprint recognition.
- Consider implementing (a) password monitoring to screen for weak, commonly used, expected, and compromised passwords, or (b) password managers/vaults to help generate complex and unique passwords for various systems that employees can easily access through a strong master password.
- Configure systems to prevent users from repeating the same password within a specified timeframe in the event that a password needs to be reset.

- Enable a password reset function on your systems so that staff members can change forgotten passwords once their identities are authenticated.
- Implement an account lockout function that triggers after a certain number of failed attempts and set accounts to automatically disable if they are inactive for a predefined amount of time.
- On devices or systems that have optional password protection, make sure to enable this feature.

## Password Don'ts

- Advise staff members to avoid passwords or passphrases that:
  - Contain common words or terms, even if the spelling is slightly altered (example: Practic31234 or Chir01234).
  - Use common phrases, famous quotations, and song lyrics (e.g., 2BeOrNot2Be?).
  - Contain personal information, such as first, middle, or last names; pets' names; street names; Social Security numbers; etc. (example: JaneDoe1975).
  - Are overly simplistic or easily guessed (example: PassWord1234).
  - Use adjacent keyboard combinations (example: qwerty1234).
  - Contain pop culture references (example: \$tarWar\$2024).
  - Use information found on social media sites (example: @JaneDoeTweets).
- Avoid systems that use password hints or knowledge-based authentication (KBA) as a method of password recovery. Evidence suggests hints often are weak password forms (example: favorite science fiction movie), and KBA selections can be easily guessed or researched (example: mother's maiden name).

- Advise staff to not write down passwords as a method of remembering them, even if they think they are concealed.
- As part of security policies, prohibit staff from sharing passwords with other personnel or letting others use a system or network while they are logged in.
- Recommend that staff do not use the same password for multiple systems and personal/professional accounts.

## In Summary

Although no strategy can guarantee complete protection, following best practices for password security and avoiding known password vulnerabilities can improve your practice's ability to defend against cyberattacks and data breaches.

Cybersecurity is an issue that will continue to evolve and present challenges in chiropractic care. As hackers hone their password-cracking skills with emerging tools and technologies, implementing emerging best practices for password security will be an essential part of chiropractic practices' security protocols and staff education priorities.

To learn more about safeguarding systems and data, see the curated links in [MedPro's Risk Resources: Cybersecurity](#).

## Endnotes

<sup>1</sup> Davis, J. (2020, September 2). Healthcare's password problem and the need for management, vaults. *Health IT Security*. Retrieved from <https://healthitsecurity.com/news/healthcares-password-problem-and-the-need-for-management-vaults>

<sup>2</sup> Cybersecurity & Infrastructure Security Agency. (2020, January 21). *Security tip (ST05-012): Supplementing passwords*. Retrieved from <https://us-cert.cisa.gov/ncas/tips/ST05-012>; Davis, J., Healthcare's password problem; *HIPAA Journal*. (2021, March 9). The HIPAA password requirements and the best way to comply with them. Retrieved from [www.hipaajournal.com/hipaa-password-requirements/](http://www.hipaajournal.com/hipaa-password-requirements/); Office of the National Coordinator for

Health Information Technology. (2015, January). *Top 10 tips for cybersecurity in healthcare*. U.S. Department of Health and Human Services. Retrieved from [www.healthit.gov/sites/default/files/Top\\_10\\_Tips\\_for\\_Cybersecurity.pdf](http://www.healthit.gov/sites/default/files/Top_10_Tips_for_Cybersecurity.pdf); Office of the National Coordinator for Health Information Technology. (2010, November). *Cybersecurity: 10 best practices for the small healthcare environment*. U.S. Department of Health and Human Services. Retrieved from [www.healthit.gov/sites/default/files/basic-security-for-the-small-healthcare-practice-checklists.pdf](http://www.healthit.gov/sites/default/files/basic-security-for-the-small-healthcare-practice-checklists.pdf); Venditto, G. (2015, October). Best practices for password security. *Healthcare IT News*. Retrieved from [www.healthcareitnews.com/news/best-practices-password-security](http://www.healthcareitnews.com/news/best-practices-password-security); National Institute of Standards and Technology. (2017, June). *Digital identity guidelines* (NIST Special Publication 800-63-3). Retrieved from <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf>

<sup>3</sup> Strawbridge, G. (2021, March 2). *Password policy best practices 2021*. MetaCompliance. Retrieved from [www.metacompliance.com/blog/password-policy-best-practices-2021/](http://www.metacompliance.com/blog/password-policy-best-practices-2021/); Microsoft. (2021, July 12). *Password policy recommendations*. Retrieved from <https://docs.microsoft.com/en-us/microsoft-365/admin/misc/password-policy-recommendations?view=o365-worldwide>

*This document should not be construed as medical or legal advice. Because the facts applicable to your situation may vary, or the laws applicable in your jurisdiction may differ, please contact your attorney or other professional advisors if you have any questions related to your legal or medical obligations or rights, state or federal laws, contract interpretation, or other legal questions.*

*ChiroPreferred is the marketing name used to refer to the chiropractic-related products offered by MedPro Group. MedPro Group is the marketing name used to refer to the insurance operations of The Medical Protective Company, Princeton Insurance Company, PLICO, Inc. and MedPro RRG Risk Retention Group. All insurance products are underwritten and administered by these and other Berkshire Hathaway affiliates, including National Fire & Marine Insurance Company. Product availability is based upon business and/or regulatory approval and may differ among companies. © MedPro Group Inc. All Rights Reserved.*