External Policies and Procedures

TherapyAppointment.com

Protecting User Accounts for 2.0

Purpose

Passwords and security standards are important aspects of computer security. A poorly chosen or protected password or weak device security may result in unauthorized access and/or exploitation of TherapyAppointment's resources, your client information, and/or patient PHI. All TherapyAppointment account holders are responsible for taking the appropriate steps, as outlined below, to select and secure their application passwords and devices.

Based on mature practices and standards, TherapyAppointment's policy to protect user accounts represents minimum standards and guidelines for the application user. The policy and standards aim to provide a balance of usability and security, though they are not without practical limits. Password and device security has never been bulletproof. Users should evaluate minimum standards, evaluate risk, and incorporate the additional recommendations as appropriate for their own environment.

Scope

This policy applies to all TherapyAppointment users, including business customers and clients who use TherapyAppointment through this affiliation in order to schedule appointments or communicate with clinicians.

Policy Requirements

1.1 User Accounts

- Every user that accesses TherapyAppointment, in association with your account, must create an account with a unique username that identifies the individual within the application.
- Customers are required to provide a unique email address to which they have ongoing private access. This email address will be used as a means of communication if they fail to respond to other attempts at communication, such as system messages advising of a possible suspension of account privileges.
- Sharing login credentials and shared generic user accounts are a violation of the Terms of Services (TOS) and Business Associate Agreement (BAA). Each user of the TherapyAppointment system must have separate and unique access credentials.
- Accounts that are reassigned from one user to another within a given role are counted as generic user accounts and a violation of the TherapyAppointment TOS and BAA.

- In the event that a user is terminated, or that emergency access is required, a practice Owner or other designated individual may be permitted temporary access to facilitate transition of records and to view recent messages from clients. Before such access is granted, the practice Owner must assert in writing that they (or the corporate entity that they represent) are the legal owners of these records, and are entitled under law to retain access to them.
    - The designated individual must also be a subscribed user of TherapyAppointment with an active user account.

1.2 How to Comply

- Verify that each workforce member has their own account, which is set up under their real identity and linked to the individual's workforce email account.
- If a clinical or administrative staff member leaves your employment, establish a new account (with a new username and password) for their replacement.

2.1 Password Strength and Hygiene

- TherapyAppointment requires that your user passwords are composed of at least 8 characters, and include characters selected from the following groups:
    - `A-Z`
    - `a-z`
    - `0-9`
- Passwords should not be based on simple or predictable patterns or values.
- Passwords may include any of the following character groups:
    - `A-Z`
    - `a-z`
    - `0-9`
    - `!@$*=+~_-`
- Do not recycle passwords that you have used in the past for other applications.
- Do not disclose your user password to any other party, including colleagues, practice Owners, or TherapyAppointment staff.
- Do not use a user password that is already known, or likely to be known, by another party.
- Do not transmit your password in email, text message, or other such communication mediums.
- Do not store unprotected copies of your password in digital or physical form.
- Clinical customers are permitted to reset forgotten passwords using the password reset functionality built into the login form.
- Clients can reset their own passwords using the functionality within the application.

2.2 How to Comply

- Choose a password you have not used before (for any purpose) to protect your TherapyAppointment account.
- Avoid using predictable patterns as the basis for your password. Do not base your password directly on a word, phrases, proper name, date, or sequence of characters appearing on a keyboard or keypad.

- Never share or publish your password. Never disclose your password to any party, known or unknown.
- Avoid storing physical copies of your password, and always protect physical copies as though they are PHI.
- Always protect electronic copies of your password as though they are PHI or other protected information.
- Advise patients about the risks of sharing accounts where PHI is sent/received and the need to select strong passwords.

2.3 Recommendations

- Use a tool, like a password manager, that helps you generate complex and unique passwords for every site or application with which you hold a user account.
    - Only use password managers that protect your secrets with strong encryption and additional layers of security.
    - Let the password management tool do the work and generate the strongest password the site will allow.
    - Turn off the default “save password” features of your web browser, e.g., Chrome or Microsoft Edge.
- If you choose to create your own passwords, remember that length is one of the best predictors of a strong password. Choose passwords consisting of 12 or more characters.
- Word-based passphrases can provide good protection if they are made up of random and unrelated words. A passphrase consisting of 5 or more words is desirable.
- Change your password periodically but not so often that you are tempted to select a predictable and weak password. Changing passwords only when you think they may have compromised may be acceptable for strong, unique passwords that aren’t used across multiple applications.

3.1 Protect Your Environment

- Maintain the security and compliance of your computing environment. These tasks are the responsibility of each business customer or other user as are incidents caused by weaknesses in this environment.
- Do not use TherapyAppointment from devices that are suspected to be infected or hacked. Neither should you access your account from a device that is missing critical software and security updates within the operating system or browser environment.
- Maintain the security of your account by locking your device when you step away and optionally logging out of TherapyAppointment.
    - Do not use public Wi-Fi when accessing data that may contain PHI or other types of personal information. Use your phone’s hotspot if you must access data in a public place, but avoid this entirely if at all possible.
- Maintain the security of your account by changing your password in response to security-related incidents, including:
    - Physical intrusion or theft
    - Malware infections

    - Unauthorized access to your email account or other sensitive accounts
    - Detection of hacking related activity
    - Accidental disclosures
- Any application user who suspects that his/her password may have been compromised must report the incident to support@therapyappointment.com or call 1-800-242-2127 and change their passwords immediately.

3.2 How to Comply

- Regularly install software updates for your computer operating system, web browser, and other applications to ensure that you have the latest security patches.
- Run a regular virus scan on your computer, using a third party scanner if needed. Change your password if a scan reports a critical infection.
- Seek professional guidance to recover devices that have been infected with malware or compromised successfully by hackers.
- Contact customer support if you suspect your password or system might have been compromised.
- Turn on a time-based screen lock on your device.
- Log out of TherapyAppointment when you will be turning your attention to other tasks.

4.1 Additional Guidance for Covered Entities

- Covered Entities should review their own responsibilities under HIPAA/HITECH and related rules. The compliance activities and safeguards undertaken by TherapyAppointment do not alleviate a customer's own responsibilities.
- Always adjust guidance based on the threats and risks that concern your practice. 12 character passwords may not be long enough. Six months might be too long to go without changing your password.
- Protect email accounts associated with your practice.
    - Use a business email account that will accept shared responsibility for the security and compliance of your email account. Do not use free accounts that are issued on domains you do not control, e.g., *some.therapist@gmail.com* or *some.therapist@hotmail.com*.
    - Learn about 2-step verification or 2-factor authentication and enable it on the email account linked to your TherapyAppointment account.
- Protect your DNS domains associated with your practice.
    - Choose a good domain registrar company (one that offers 2FA, DNS management, and technical support).
    - Enable two-factor authentication.
    - Enable domain locking.
    - Enable WHOIS protection.
    - Use a strong password.
    - Keep your domain contact details updated.
    - Be suspicious of any emails requesting domain registrar details.

    - Keep domain hosting and domain registration on separate accounts at separate companies.
- It may be important to store local backups and versions of your data for business purposes, but remember that TherapyAppointment can do little to protect that local data. It's up to you to develop a plan to manage that risk.
- Encrypt your computers and mobile devices in a manner consistent with the HIPAA Security Rule and industry recommendations. MacOS and Windows 10 Professional provide the required tools to do this and, in many cases, meet Safe Harbor requirements.
- Secure your network connections. Even though TherapyAppointment encrypts its communication with your computer, open wireless networks expose your device to malware and hacking related threats.
    - Make sure that the wireless router uses WPA2 encryption and a strong password in order to allow access.
    - Do not allow guest access to your office network, except through a dedicated Guest network that is isolated from your work environment.
    - Be cautious in deploying "Internet of Things" devices on your home or office networks. These devices are becoming frequent entry points for attacking users.

Version Control Log

Approved	Susan Whitehead	**Effective**	08/21/2019
Last Review	N/A	**Review by (Date)**	8/31/2021
Reviewed By	N/A		
Revision History			
8/21/2019	Formalized initial policy		