The Baltimore Therapy Center

Employee Handbook

Contents

Section 1. Introduction

1.1. Purpose of this Handbook

The purpose of this Handbook is to familiarize you, the employee, with the policies, rules and other key aspects of The Baltimore Therapy Center (the "Company"). The information in this handbook supersedes all rules and policies that may previously have been expressed or implied, in both written and oral format. Compliance with this Handbook is compulsory for all employees. The Company reserves the right to interpret this Handbook's content as it sees fit, and to deviate from policy when it deems necessary.

1.2 Changes of Policy

The Baltimore Therapy Center reserves the right to change this Handbook's content, at any time and at our sole discretion. Its provisions may not be altered by any other means, oral or written. You will receive written notice of any changes we make to the employee handbook and are responsible for understanding and complying with all up-to-date policies. If you are confused about any information defined herein, please contact the Human Resources Manager.

1.3 Employment Forms

All new employees are required to complete and submit the following forms:

Employment Eligibility Form I-9
On the day of hire, each new employee is legally obligated to complete the Employment Eligibility Verification Form I-9 and submit documents to verify identity and employment eligibility within the next three (3) business days. The same policy applies to re-hired employees whose I-9's are over three (3) years old or otherwise invalid.

Section 2. Terms & Definitions

The Baltimore Therapy Center typically employs less than 20 employees regular and temporary employees on an "at-will" basis. This section defines the terms of "at-will" employment, as well as the different types of employees we hire.

2.1 Definition of "At-Will" Employment

The job of an "at-will" employee is not guaranteed. It may be ended, at any time and with or without notice, by the employee or, for a lawful reason, by the Company. The Company also reserves the right to alter an "at-will" employee's benefits, pay rate, and assignments as it sees fit. The "at-will" terms of employment may only be changed with the approval of the Director, and must be signed off by the Director.

2.2 Types of Worker

This section distinguishes between the different types of workers the Company employs. Employee status is established at the time of hire and may only be altered via a written statement signed by the Company.

Exempt vs Non-Exempt

Most employees are non-exempt, meaning they are entitled by law to at least minimum wage and premium pay for overtime. Exempt employees are not subject to these laws. Exempt status is defined by standards set by state law and the Federal Labor Standards Act (FLSA). This class of employee is usually an executive, an administrator, or a highly paid specialist such as a programmer.

Regular vs. Temporary

Regular employees work a regular schedule, either on a full-time or part-time basis. To be considered full-time, an employee must work at least 40 hours per week. A temporary employee is a person we hire for a short period (usually 3 months at maximum) to assist with a project or remedy a staff shortage. A temporary employee is also employed on an "at-will" basis (defined above).

Independent Contractors & Consultants

Independent contractors and consultants are not Company employees, but rather self-employed professionals whom we hire for specific projects. Unlike employees, they do not operate under Company direction, and control their own methods, materials and schedules. They are not eligible for Company benefits.

Section 3. Payroll

3.1 Timekeeping

It is the policy of the Company to maintain a timekeeping system that complies with the FAR and the DCAA requirements as follows:

A timesheet must be made out on a daily basis by the employee. If a change is made on a timesheet, it must be made by the employee and a reason must be provided for the change. The timesheet must identify the project or activity the employee is working on.

The employee must account for all time worked whether compensated or not. The timesheet must be signed by the employee as true and correct. The supervisor must approve the employee’s entire timesheet, including any changes to a timesheet.

3.2 Payment Schedule

Employees are paid twice a month generally on the 1st and the 15th of the month. In cases where the regular payday falls on a holiday, Employees will receive payment on the last business day before said holiday.

3.3 Wages

Wages vary from employee to employee and are based on level of skill and experience. The Company conducts regular evaluations of all employees and issues promotions as it sees fit. Employees who feel

entitled to higher pay may contact the Director to discuss. In addition to regular pay, employees may have the option of earning overtime pay and/or bonuses.

Overtime

A non-exempt employee may work overtime on the terms defined by Maryland law pending prior authorization by his or her manager.

3.4 Deductions & Garnishment

Deductions

Federal and state law requires that we deduct the following from every paycheck:

- Social Security
- Income tax (federal and state)
- Medicare
- State Disability Insurance & Family Temporary Disability Insurance
- Other deductions required by law or requested by the employee

A Wage and Tax Statement (W-2) recording the previous year's wages and deductions will be provided at the beginning of each calendar year. If at any time you wish to adjust your income tax withholding, please fill out the designated form and submit it to Accounting.

Wage Garnishment

Sometimes, the Company receives legal papers that compel us to garnish an employee's paycheck – that is, submit a portion of said paycheck in payment of an outstanding debt of the Employee. We must, by law, abide by this either until ordered otherwise by the court or until the debt is repaid in full through withheld payments or otherwise.

Section 4. Rights & Policies

The following section summarizes your legal rights as an employee of The Baltimore Therapy Center. Questions about any policy detailed in this section may be addressed with a Human Resources representative.

4.1 Equal Opportunity Employment Policy

The Company provides equal employment opportunities to all applicants, without regard to unlawful considerations of or discrimination against race, religion, creed, color, nationality, sex, sexual orientation, gender identity, age, ancestry, physical or mental disability, medical condition or characteristics, marital status, or any other classification prohibited by applicable local, state or federal laws. This policy is applicable to hiring, termination and promotion; compensation; schedules and job assignments; discipline; training; working conditions, and all other aspects of employment with the Baltimore Therapy Center. As an employee, you are expected to honor this policy and to take an active role in keeping harassment and discrimination out of the workplace.

4.2 Accommodation for Disabled Employees

We are happy to work with otherwise qualified disabled employees in order to accommodate limitations, in accordance with the Americans with Disabilities Act (ADA). It is up to the employee to approach his or her supervisor with this request, and to provide medical proof of his or her needs upon the Company's request. We are also happy to accommodate employees diagnosed with life-threatening illnesses. Such employees are welcome to maintain a normal work schedule if they so desire, provided that we receive medical papers proving their working cannot harm themselves or others and their work remains at acceptable standards.

4.3 Employment of Minors

Our policy on employment of minors adheres to all FLSA standards, including the following:

- Minimum employment age (14 for non-agricultural work)
- Maximum weekly hours for employees under 16
- Minimum hazardous job employment age (18)
- Minimum wage standards for students, apprentices, disabled employees, and employees under the age of 20.

4.4 Employment of Relatives

The employment of relatives can prove problematic, particularly in situations where relatives share a department or a hierarchical relationship. The Company will not hire relatives to work in any potentially disruptive situation. An employee must inform us if he or she becomes a co-worker's relative. If at any time we perceive the situation to be dysfunctional, we may have to reassign or ask for one relative's resignation in order to remedy the situation.

4.5 Religion & Politics

The Baltimore Therapy Center is respectful of all employees' religious affiliations and political views. We ask that if you choose to participate in a political action, you do not associate the Company in any way. We are happy to work with employees to accommodate political and religious obligations, provided accommodations are requested from a manager in advance.

4.6 Private Information

Employee information is considered to be private and only accessed on a need-to-know basis. Your healthcare information is completely confidential unless you choose to share it. In some cases, employees and management may receive guidelines ensuring adherence to the Health Insurance Portability and Accountability Act (HIPAA). Personnel files and payroll records are confidential and may only be accessed for legitimate reasons. If you wish to view your files, you must set up an appointment in advance with Human Resources. A Company-appointed record keeper must be present during the viewing. You may only make photocopies of documents bearing your signature, and written authorization is needed to remove a file from Company premises. You may not alter your files, although you may add comments to items of dispute. Certain information, such as dates of employment and rehiring eligibility, are available by request only. We will not release information regarding your compensation without your written permission.

4.7 Leaves of Absence

Employees requiring time off from work may apply for a leave of absence. All leaves must be approved by management. For planned leaves, employees must submit requests at least 5 days in advance. Emergency leaves must be requested as soon as possible. Accepting/performing another job or applying for unemployment benefits during leave will be considered voluntary resignation. We consider all requests in terms of effect on the Company and reserve the right to approve or deny requests at will, except when otherwise directed by law. Any request for a leave of absence due to disability will be subject to an interactive review. A medical leave request must be supported in a timely manner by a certification from the employee's healthcare provider. Extension of leave must be requested and approved before the current leave ends. No employee is guaranteed reinstatement upon returning from leave, unless the law states otherwise. However, the Company will try to reinstate each returning employee in his or her old position, or one that is comparable. Below are the three main types of leave that The Baltimore Therapy Center offers employees. Some, but not all, are governed by law.

Work-Related Sickness & Injury

Employees eligible for Worker's Compensation rendered unable to work because of a work-related injury or illness will receive an unpaid leave for the period required. For eligible employees, the first 12 weeks will be treated concurrently as a family and medical leave under FMLA.

Maternity

An employee disabled on account of pregnancy, childbirth, or a related medical condition may request an unpaid leave of absence of up to four months. Time off may be requested for prenatal care, severe morning sickness, doctor-ordered bed rest and recovery from childbirth.

Election Days

Provided an employee's schedule does not allow time for voting outside of work, and that he/she is a registered voter, he/she may take up to two hours, with pay, at the beginning or end of a workday, to vote in local, state or national elections.

Vacation Policy

Full-time employees are allotted 10 days of paid vacation per year. Unused vacation days may be carried over and used for a period of one year. From the 5th year of service employees are allotted 20 days of paid vacation per year.

Section 5. Employment Benefits

5.1 Unemployment Insurance

Employees rendered unemployed through no fault of their own or due to circumstances prescribed by law, and who meet the State eligibility requirements for time worked or wages earned, may receive unemployment insurance (also called unemployment benefits or compensation). State agencies directly administer this insurance and determine benefit eligibility, amount (if any), and duration.

5.2 Workers' Compensation

Workers' Compensation laws compensate for accidental injuries, death and occupational disabilities suffered in the course of employment. The Baltimore Therapy Center provides Workers' Compensation Insurance for all employees. Generally, this includes lost wages, disability payments and hospital, medical and surgical expenses (paid directly to hospital/physician) and assistance for injured employees in returning to suitable employment.

5.3 Social Security Benefits (FICA)

Both employees and the Company contribute funds to the federal Social Security Program as prescribed by law, providing retirees with benefit payments and medical coverage where applicable.

Section 6. Rules of Conduct

6.1 On the Job

Reporting for Work

Employees are expected to begin and end each shift at the time and on the day appointed. You must inform your supervisor before the start of the workday if you will be absent or late and obtain his or her permission to leave early. Absences and late arrivals will be recorded. Should your absences or tardiness exceed 3 latenesses in a 30-day period or 3 unexcused absences in a 6-month period, you will be subject to disciplinary action and possible termination. Failing to call one's supervisor or report to work for consecutive workdays will be considered voluntary resignation and result in removal from payroll.

Staying Safe

Safety in the workplace is the Company's number one priority. You must inform your supervisor in the event of unsafe conditions, accident or injury, and use safe working methods at all times.

Meals & Breaks

Unless defined otherwise by Maryland state law, non-exempt employees are entitled to a paid 10-minute break for every four hours of work, as well as a 30-minute meal break for any shift lasting longer than five hours.

Social Media Policy

The Baltimore Therapy Center recognizes the importance and relevance of social media and its benefits. However, the company must protect its professional image and guard any intellectual property rights. Thus, we encourage employees to refrain from using their personal social networking channel to discuss the Baltimore Therapy Center.

When referring to our Company in any way, employees must always conduct themselves in a professional manner and must respect the views and opinions of others. Behavior and content that may be deemed disrespectful, dishonest, offensive, harassing or damaging to the Company's interests or reputation are not allowed and will not be tolerated. The use of social media channels on company time for personal purposes is not allowed. Employees must not disclose private or confidential information about the Company, its employees, clients, suppliers or customers on social networks. The Company

reserves the right to monitor company-related employee activity in social media networks; violations of this policy are grounds for discipline in the Company's sole discretion.

Cell Phone Use

Cell phones brought to work must be on silent or vibrate mode to avoid disrupting coworkers. They may only be used during breaks and meal periods, away from where others are working. If cell phone use interferes with operations in any way, an employee's cell phone privilege may be rescinded and disciplinary action, up to and including termination, may be used. Employees who receive Company devices may use them for Company business only. All phones must be silenced during meetings and client sessions.

6.2 Rules & Policies

Confidentiality

No previous or current employee may disclose or give access to confidential Company information, in any way or at any time, unless otherwise authorized by Management.

Discrimination & Harassment

In keeping with our Equal Opportunity Employment clause, the Company will not tolerate on-site discrimination or harassment on any legally protected basis, including that of physical characteristics, mental characteristics, race, religious or political views, nationality, disability, medical condition, sex, sexual preference, or gender identification. Harassment and discriminatory behavior among employees or contractors will result in disciplinary action, with the possibility of termination. Discrimination and harassment by customers or other business associates should be immediately reported to your supervisor, at which point the Company will investigate and take corrective action. In the even that you are uncomfortable reporting to your direct supervisor you may also report any discrimination or harassment to the Director of the Baltimore Therapy Center.

You are welcome to seek legal relief if you find the Company's actions inadequate.

Drugs & Alcohol

Good performance on the part of our employees is crucial to The Baltimore Therapy Center's success. For this reason, we strictly forbid employees to do the following while at work (including any part of Company property, Company vehicles, and during work hours):

- Drinking alcohol and selling, purchasing or using illegal drugs at work. An "illegal drug" is any drug that has not been obtained by legal means. This includes prescription drugs being used for non-prescribed purposes.
- Possession of any non-prescribed controlled substance, including alcohol and legal but illegally obtained prescription drugs.
- Reporting for work intoxicated. We reserve the right to test employees for substance abuse.

Illegal drugs, illegal drug metabolites, or excessive alcohol in your system will result in disciplinary action up to and including termination. The Company cares about the overall health and well-being of its employees. Any employee who feels that he/she is developing a substance abuse problem is urged to

seek help. The Company will grant time off (within reason) for rehabilitation. Be advised, however, that this will not excuse a substance-related offense. In some cases, completion of Company-approved rehabilitation program may serve as an alternative to termination.

Dress Code

The Baltimore Therapy Center requires employees to dress in a professional and appropriate manner, i.e., business casual attire, when reporting for work.

6.3 Disciplinary Action

The Company takes disciplinary matters very seriously and will exact discipline as it sees fit for any unacceptable action or behavior. These may include:

- Excessive lateness and/or absence
- Improper or indecent conduct
- Poor communication
- Uncooperative attitude
- Abuse, perfunctory or unauthorized use, or unauthorized possession of Company property
- Unauthorized use or disclosure of Company information
- Possession and/or use of illegal drugs, weapons or explosives
- Illegal harassment and/or discrimination - of any kind
- Violations of Company policy

Disciplinary action may consist of anything from verbal/written warnings and counseling, to demotion, transfer, suspension or termination. Please review and internalize the list of "Don'ts" above and try to use good judgment at all times.

Workplace Inspections

At the Baltimore Therapy Center we have a responsibility to protect our employees and our property. For this reason, we reserve the right to inspect the following, at any time, with or without notice:

- Offices
- Computers and other equipment
- Company vehicles
- Any personal possessions brought onto Company premises, such as handbags, briefcases, and vehicles.

All inspections are compulsory. Those who resist inspection may be denied access to Company premises and be subject to disciplinary action.

Section 7. Policies specific to Private Practice

7.1 Clients arriving late/no-shows

When a client does not show up on time, the employee should reach out by phone (or text, if a request for nonsecure communications has been made) at 10 minutes after the designated start time.

If the client responds that they will be coming to the session (or wish to meet online instead of meeting in person if that was the original plan), the employee should remain at the office or by their device and wait until the end of the session time. If the client shows up, the employee may, but is not required to, go beyond the planned end time of the session. They will be paid for a full hour of time.

If the client does not respond, the employee should reach out by phone at 20 minutes after the designated start time and leave a message if the call is not picked up. The employee should wait 5 more minutes and then may leave. They will be paid for half an hour.

7.2 Late cancellations

When a client cancels less than 24 hours before a session, the policy of the practice is to charge the client the full session fee. The employee may at their discretion agree to reschedule the session and not charge the client.

7.3 Documenting outreach efforts

For clients who are being paid for by a third party (e.g. Department of Social Services), it is important to document our efforts to provide services. Thus, employees should use the client outreach log to document calls/emails/texts sent to clients for scheduling purposes and note if they were not able to reach the client, if messages have been left, etc., so that we can demonstrate that we made appropriate efforts.

Section 8. Baltimore Therapy Center Security Policy

Please refer to the attached Security Policies for guidelines concerning the use of computers and technology.

Version: 1.0

Approved By: Raffi Bilek

Effective Date: 11/5/21

Table of Contents

7. The Security of Office Spaces
    - Restricted and public areas
    - Securing sensitive equipment and documents
    - Managing keys and door codes.
    - WiFi and other Internet access
8. Security Incidents
    - How to report an incident
    - How to recognize an "incident"
9. Rules for Strong Passwords and Other Forms of Authentication

1. About Baltimore Therapy Center's Security Program

Who to get help and instruction from

The following people are in charge of certain areas of Baltimore Therapy Center's security program. you may go to them for guidance on any questions related to the program. You must also follow their instructions regarding security activities and duties in your work.

It's important to remember that any changes to security measures, or to digital technology choices/settings/configurations, have to ultimately be made by or approved by the Security Officer. So if you have a need or desire for something related to Baltimore Therapy Center's security and/or technology setup, please speak with the Security Officer.

Security Officer (ultimately in charge of the security program): Raffi Bilek

Privacy Officer (ultimately in charge of decisions regarding the privacy of information): Raffi Bilek

IT Officer (in charge of monitoring technology selection, configuration, usage & maintenance): Raffi Bilek

Deputy Security Officer: Chantelle Prince

Where to find forms, policies, and other security documents you might need

This manual is meant to help you understand those aspects of Baltimore Therapy Center's security policies which you need to be familiar with for your work. **This is not the full set of official policies, however. If you need to reference them for any reason, the full set of currently active security policies which apply to your work can be found in the shared Security Policy folder.**

You will also likely need to access security-related forms from time-to-time. Except where otherwise noted in this manual, all security-related forms can be found in a subfolder the Security Policy folder.

Getting started (aka "onboarding")

When starting up at Baltimore Therapy Center, you will need to perform some onboarding tasks to get you up to speed with the security program. The Security Officer will help you complete the following onboarding tasks:

- Read this manual.

- Complete HIPAA Basics and BYOD training.
- Sign the workforce security agreement
- Receive any codes and passwords needed.
- Audit and register all personal devices you wish to use for practice business.

Training and security reminders

From time-to-time, the practice will conduct formal security trainings. You may be required to attend some or all of these, depending on your work role.

The Security Officer will also issue, on a regular basis, "security reminders." These may take many forms, such as short emails, postings in private areas of the office, or other methods of getting information to you.

It is very important that you pay close attention to the contents of these trainings and reminders. They are an integral part of how the security program stays up-to-date and communicates the breadth of information we all need to know in order to maintain the security of the practice and our clients.

Exiting the practice (aka "offboarding")

One day, you may leave Baltimore Therapy Center and move on to other things. When that occurs, the Security Officer will help you complete the following offboarding tasks:

- Scrub practice information from your personal devices and terminate their registration.
- Close your accounts in Google Workspace and/or Microsoft 365.
- Return any keys you were issued.
- Return any devices or documents you were issued.

Consequences when policies are not followed

Baltimore Therapy Center adopted its security policies to protect both clients and the practice -- including you and the other staff who work in it. In order to ensure that everyone follows these policies, Baltimore Therapy Center has adopted a Sanction Policy which describes the consequences when policies are not followed.

You should also know that these security policies were designed to help us comply with state and federal laws, including HIPAA. If anyone on staff were to violate these policies or the laws they are meant to help us comply with, there may be additional, personal legal penalties over and beyond what is defined in the Baltimore Therapy Center's Sanction Policy.

If you have any questions about the Sanction Policy, possible legal ramifications for violating policies or laws, or how to make sure you're upholding Baltimore Therapy Center's security policies, please don't hesitate to ask the Security Officer or another member of the leadership team.

2. General Security and Privacy Considerations

What This Section Is About

The practice's security policies are written to provide guidance and describe what we do to protect the security of client information. That said, there are a number of general good practices to be considered along with those policies. This section describes several of those good practices and relates to them concepts of "confidentiality, integrity, and availability."

Security Policies Covered in This Section

This section covers general HIPAA rules and ethical standards, and is not related to any specific security policy.

Why our program works the way it does

The Baltimore Therapy Center's security program is designed to:

- Protect the practice and its clients from the kinds of harm that can result from breaches of those clients' privacy or the loss of their accurate health care information.
- Adhere to the ethical standards of the major mental health professional associations.
- Comply with a federal security & privacy regulation called HIPAA, as well as state and local laws that govern health care security & privacy.

The kinds of harm that can impact clients include things like social stigma, personal/family rifts, professional stigmas that impact career and work, identity theft, insurance fraud, inability to acquire their health care records, inaccurate or incomplete records, and others.

The kinds of harm that can impact Baltimore Therapy Center include things like ruptured therapeutic alliances, loss of trust from clients and the public, malpractice cases, fines or other enforcement actions resulting from violations of HIPAA and/or state and local data privacy laws, and others.

HIPAA clearly defines three aspects of client information which we endeavor to protect. Protecting these three aspects of information is our core objective when choosing security measures for Baltimore Therapy Center's operations:

- **CONFIDENTIALITY: the privacy of client information. Clients' stories are their own to tell, and they share their stories and personal information with us under an agreement of deep trust. We must not only respect their ownership of their own information, we must also proactively work to protect their ability to choose how their information is used or not (with certain particular limitations, such as when mandatory reporting requirements arise).**
- **AVAILABILITY: client information is not lost or destroyed until the appropriate time, and it is available to us or to our clients when it is needed. We must keep documents and data safe from damage or loss, and use backups when necessary. We must also keep client information "in the circle" of the practice's own systems and equipment so that it can be found when it is**

needed. When it is time to destroy old client records, the practice will have a process for doing so properly and intentionally.

- **INTEGRITY: information is kept intact and not changed in ways that aren't closely tracked. We must keep careful records of how client information gets updated, so that we can see what changes were made and when. Client record entries must not be edited after they are signed/locked.**

Top ways to protect our clients' confidentiality

- **Don't talk about clients when you don't need to.**
- **Compartmentalize what you know about clients from other events in your life.**
- **Keep documents and screens hidden from the sight of others.**
- **Never talk about clients in any social media context.**
- **Don't talk about clients in emails/texts/etc. when there isn't a specific and approved reason to do so.**
- **Watch where you're working on practice business -- be mindful of confidentiality risks when working in public spaces.**
- **Maintain good security practices for devices, services, and documents.**

Top ways to protect the availability of our clients' information

- **Use practice services and not personal ones to do practice business.**
- **Don't delete, throw away, or shred any information about clients unless the Security Officer approves it -- even if it doesn't seem to matter.**
- **Follow the procedures that the Security Officer lays out for using practice services -- they may be essential to making sure information stays available and/or gets backed up properly.**
- **Make sure documents and devices are physically locked up (or carried in your own hands) when not in use and when you step away from them.**
- **Make sure equipment and documents are kept out of vulnerable situations, such as being placed near liquids (e.g. drink cups) or fire hazards.**
- **Maintain good security practices for devices, services, and documents.**

Top ways to protect the integrity of our clients' information

- Don't edit client information unless editing is part of a practice process. If you need to amend a client record, write an amending entry instead of editing the original.
- Maintain good security practices for devices, services, and documents.

Keeping information "in the circle"

A huge piece of keeping client information secure boils down to keeping it "in the circle." That phrase refers to the idea that the Baltimore Therapy Center maintains a secure "circle" of services, facilities, equipment, and people for holding clients and their information safe.

Many of the rules defined below will refer to this concept. It also serves as a general guiding rule for you when making decisions about where to store information, what services to use for communicating information, when and where to talk about clients or the practice, and any other activities you may engage in around the sensitive information that the Baltimore Therapy Center handles.

Always strive to keep information "in the circle" so that the Baltimore Therapy Center can ensure it stays private and can find and access the information when it is needed.

3. The Security of Sensitive Documents

What This Section Is About

When we say "documents," we mean hardcopy documents that do contain or might contain any information at all about clients or that might simply contain sensitive information. *This includes mail and packages*. It also includes free-floating paper, paper kept in folders, etc.

This section is about basic day-to-day policies for making sure documents stay confidential and don't get lost or damaged.

Security Policies Covered in This Section

This section covers essential information from the following security policies. You can find the current version of these policies in the shared Security Policy folder.

- Device and Document Transport and Storage Policy
- Facility/Office Access and Physical Security Policy

Storing sensitive documents

Any documents containing PHI should be scanned into the cloud (Google Drive/OneDrive) and immediately shredded. (Workforce members at the Baltimore Therapy Center main office who do not have a secured smartphone should place documents containing PHI in the locked mailbox.) No documents should be stored on site beyond the time that the staff member using them receives and uses them.

When a document is not actively being used by a staff member, it needs to be stored away. Documents shouldn't be allowed to sit out unless they are in the presence of a staff member. In such cases, make sure to position any sitting documents so that information on them isn't visible to onlookers.

When being stored (i.e. not actively being used by a staff member), documents containing client information need to be kept in a locked container which is, itself, also in a secure area. Health care professionals often refer to this as the "double lock."

The locked container could be in an *authorized persons only* area of the office (see "The Security of Office Spaces" below), or the space it is in could simply be protected from public access by a locked door. Alternatively, the locked container can simply be in the same space as a staff member.

For example: keeping documents in a locked drawer in a locked room would suffice. If a staff member is present in the room, the room may be unlocked. If the staff member leaves the room for only a couple minutes (e.g. to get some tea from the waiting room), the room may remain unlocked so long as the drawer is locked. If the staff member leaves for more than a couple minutes (e.g. to use the restroom or for a longer trip), both the drawer and the room need to be locked first.

Transporting sensitive documents

First, **we need to avoid transporting documents outside of office facilities where possible.** Compared to information kept on well-secured electronic devices, information kept on documents is more prone to loss or confidentiality breach when being transported.

Unless instructed to transport documents, you need to get the permission of the Security Officer before doing so.

When you do transport documents, they need to be kept in your physical possession the whole time. So if you stop somewhere on your way, carry the documents with you (preferably in a bag or case, of course.) **Do not leave documents in the car -- not even in the trunk (data shows that the trunk is not as secure for this purpose as we might like it to be.)**

Destroying sensitive documents

First, documents should only be destroyed according to practice policies or according to the instruction of the Security Officer or other practice official. While clinicians generally know when it is legal for client records to be destroyed, document destruction needs to be done according to the practice's policies and procedures.

Documents should be destroyed using the shredders and disposal equipment supplied by the practice.

When placing documents in boxes/bins/etc. to be shredded later, make sure the document is fully inserted into the container so that it cannot be pulled out or seen by another person, and that the container is locked when you leave it.

4. The Security of Computing and Storage Devices (Including Your Own)

What This Section Is About

This section is about the security of client information that is stored on -- and also accessed through -- computers, smartphones, thumb drives, external hard drives, CDs, floppy disks, and any other devices or media that do computing or that just store electronic info.

This section will lay out the basic rules you need to follow for keeping these devices away from people who shouldn't have access to them and for protecting them from virus and malware infections. It also lays out rules for making sure *the information the devices store or access* is kept away from people who shouldn't get access to it (*confidentiality of information*), and that the information doesn't get lost or put in places where practice administrators can't find it (*availability and integrity of information*.)

Security Policies Covered in This Section

This section covers essential information from the following security policies. You can find the current version of these policies in the shared Security Policy folder.

- Computing Devices and Electronic Media Technical Security Policy
- Passwords and Other Digital Authentication Policy
- Computing Devices Acceptable Use Policy
- Bring Your Own Device Policy
- Data Backup Policy
- Device and Document Disposal Policy
- Device and Document Transport and Storage Policy
- Facility/Office Network Security Policy

Using Your Personal Devices (BYOD -- Bring Your Own Device)

The practice allows staff to use personal devices according to the rules of the Bring Your Own Device Policy. That policy requires you to *register* any devices you wish to use for any practice business of any kind, and to ensure that the devices meet the security standards of the practice.

Devices provided by Montgomery County are managed by their IT department, and workforce members are to follow their policies. The County is responsible for overseeing such devices and when in doubt, workforce members should fall back on the Baltimore Therapy Center's practices and policies.

To successfully register your personal devices, they will all need to meet certain technical requirements. Baltimore Therapy Center's BYOD (Bring Your Own Device) instructional resources provide checklists and tutorials for securing devices to the practice's standards. The Security Officer can help you find these resources and get your devices ready for a successful registration process.

If a device of yours is unable to meet any of the technical requirements, for whatever reason, then we cannot register it and it cannot be used for practice business. The risks of working with unsecured devices are simply too high.

You will not have to become an IT expert in order to keep your devices registered. You will, however, have to make sure you do not disable any of these measures for as long as your device is registered with Baltimore Therapy Center.

While there are other resources for completing device registration, here we will list the technical measures required for all registered personal devices:

- FULL-DEVICE ENCRYPTION (FDE). FDE does amazing things to protect the confidentiality of information stored on your registered devices. If you are registering a Windows computer, you may have to upgrade your Windows operating system software to accommodate this requirement. Otherwise, all commercial electronic devices should have the ability to perform FDE.
- A DEVICE PASSWORD THAT MEETS THE PRACTICE'S STANDARDS FOR STRONG PASSWORDS. See below for the practice's password standards.

- ACTIVE ANTIVIRUS/ANTIMALWARE SOFTWARE. Yes, even on Macs. But iPhones/iPads and Chromebooks are a special exception.
- AN ACTIVE FIREWALL. Once again, iPhones/iPads and Chromebooks are a special exception.
- A SEPARATE USER ACCOUNT FOR PRACTICE BUSINESS. Not all devices can support multiple user accounts. But for the ones that do, you'll need to make an account for doing practice business that is separate from your personal account.
- AUTOLOCK/AUTO-LOGOUT. If your device goes to a lock screen after being left idle for a bit, that helps keep the honest people honest. And we like doing that.
- PREVENT SYNCHRONIZATION OF CLIENT INFORMATION WITH PERSONAL SERVICES. Pretty much every device likes to be "helpful" and send your data up to iCloud/Google/Microsoft. You need to make sure that client info isn't being sent like this.
- BACKUPS, IF IT'S NEEDED. Personal devices should not usually need backups for client information. But if yours does, you'll need a Security Officer-approved backup strategy.
- UPDATED OPERATING SYSTEM SOFTWARE. You'll be expected to keep all registered devices' operating software up to date.

Smartphones are also expected to have active **remote tracking** and **remote wipe**.

There are also behavioral safety requirements for registered devices. You will be expected to treat your registered personal devices with the same attention to security with which you would treat a device owned by the practice. That includes the following behaviors:

- Carrying your registered devices with you when transporting them. This includes keeping computers and phones with you rather than putting them in the trunk of your car while you make a stop between the office and home. It also includes bringing computers and phones with you when you get up from the table at a coffee shop, restaurant, or other public place (yes, even if you are going to the bathroom!)
- Not lending your registered phone to a stranger, even if they really need to make a call.
- Not using your registered devices to do risky things, such as surfing pornographic websites or illegal download sites. Another risky behavior is downloading and installing unknown software or opening unknown files.
- Connecting your registered devices only to the WiFi networks or other Internet connections that are listed below as acceptable for practice devices and registered personal devices, *unless* you are using a VPN (as with County-provided laptops). Using a personal cellular hotspot is acceptable. In fact, personal cellular hotspot devices are not required to be registered with the practice!
- Keeping the security settings on the device as they are. If there arises a reason why you might need to disable a security setting or security measure, consult with the Security Officer on how to do so in a manner that keeps the device and its PHI secure.

When you wish to cease using a device for practice business -- maybe because you're getting rid of it, or because you simply wish to divorce it from the practice's business -- you will need to "retire" it from the practice by removing all practice information from it and by terminating the device's registration. The

Security Officer can help you find termination forms and perform the process of removing practice information from devices in a way that adheres to the practice's security policies.

Using the Practice's Devices

When using computers or other devices that belong to the practice, or to contractual partners of the practice (e.g., Montgomery County), there are certain rules for using them in a way that protects clients and also protects the practice. The following bullets are an excerpt from the Computing Devices Acceptable Use Policy.

- Installation of new software or apps must be limited to software which is approved by the Security Officer, or to apps that are downloaded from the Apple App Store/iTunes (for iOS apps) or from any of Google's repositories (for Android apps.)
- Devices must not be used to access websites that are more likely than usual to deliver malware to visitors. These sites include but are not limited to pornographic websites, illegal file sharing websites, and websites with elements intended to deceive the reader into clicking links or buttons they don't intend to click.
- When using devices to access email, text messages, or other messaging services, the user must not click any links or follow any directions contained in unsolicited messages. In other words, users must not click the links or follow the directions in spam, phishing messages, or any other message whose sender is not already known. When unsure whether or not to ignore a message from an unknown sender, users should consult with the Security Officer or other designated person.
- Practice devices may not be used at any time to:
    - Access or use client information for purposes other than those necessary for normal provision of services.
    - Copy protected health information or proprietary information belonging to the practice unless necessary for the practice's normal operations or as directed by an authorized manager of the practice.
    - Store or transmit illicit materials.
    - Harass others.

The same behavioral safety requirements that apply to registered personal devices as described above apply to practice-owned devices as well:

- **Carrying practice-owned devices with you when transporting them. This includes keeping computers and phones with you rather than putting them in the trunk of your car while you make a stop between the office and home. It also includes bringing computers and phones with you when you get up from the table at a coffee shop, restaurant, or other public place (yes, even if you are going to the bathroom!)**
- **Not using your practice-owned devices to do risky things, such as surfing pornographic websites or illegal download sites. Another risky behavior is downloading and installing unknown software or opening unknown files. No software may be downloaded without permission from the Security Officer.**

- **Connecting your practice-owned devices only to the WiFi networks or other Internet connections that are listed below as acceptable for practice devices and registered personal devices. Using a personal cellular hotspot is acceptable. In fact, personal cellular hotspot devices are not required to be registered with the practice!**
- **Keeping the security settings on the device as they are. If there arises a reason why you might need to disable a security setting or security measure, consult with the Security Officer on how to do so in a manner that keeps the device and its PHI secure.**

Practice-owned devices have the following added requirements:

- **Practice-owned devices may be used for the work purposes only, and only for the work purposes of the Baltimore Therapy Center. Note that there is no expectation of individual privacy on a practice-owned device.**
- **Nobody except the employee to whom the device was given may use the device for any purpose.**

In addition to the items above, it is very important that you do not disable any security settings on practice devices. If anything arises that leads you to believe that a security setting needs to be changed or deactivated, consult with the Security Officer rather than making changes by yourself.

You will be expected to return the device in the condition you received it, minus normal wear and tear. If you damage or lose the device, you will be responsible for the cost of replacement. If any problems with the device arise, you must report it to the Security Officer immediately.

Considerations on where you use devices

When using any device for practice business, be mindful of the context around you. Performing practice business in public -- or even in your own home -- brings certain confidentiality risks with it.

People behind you may be able to view your screen. Remember that “shoulder surfing” is not just an activity for people with malicious intent. Even “honest” people may find themselves reading your screen if the opportunity arises. Positioning your screen to avoid being viewed by others is not only a service to our clients and the practice, but it is also a service to the people around you.

When using the phone or video services, others may be able to hear you. Private spaces with sufficient sound dampening should always be used when on any type of call where clients or client information might be discussed.

Lastly, it is very important that you only use WiFi or other Internet connections that are trusted by the practice. See below for more details.

WiFi and Other Internet Connections

When we connect a device to WiFi, it is like swimming in a lagoon with all the other devices connected to the same WiFi. Even connecting to “secure” WiFi can result in your device getting a virus or being

"cloned" by a malicious WiFi lagoon swimmer. For this reason, any registered personal device or practice device may only be connected to approved WiFi networks.

Your home WiFi is approved for such devices if it uses WPA2 Personal (or better) security and the WiFi router is in your own control and is physically protected from tampering by people other than you and your family. **WiFi shared with an apartment building or "shared" with the neighbor is not to be connected with -- it is simply too risky for clients and the practice.**

You may connect registered personal devices and practice devices to personal cellular connections. That means it is both acceptable and encouraged to use the data service on your smartphone for practice business. Using your smartphone as a cellular WiFi hotspot is an encouraged alternative to connecting to untrusted WiFi. If you have a device that is used purely for setting up a *personal* cellular WiFi connection, it may be used even if it is not registered with the practice. You need to keep such devices in your own possession at all times, however.

The Security Officer has compiled a list of WiFi networks which are acceptable to connect with:

- Your home WiFi network that meets the standards described above.
- Your own cellular data/personal cellular WiFi hotspots.
- The WiFi network at the Baltimore Therapy Center's office.
- If using a VPN setup that has been approved by the Security Officer as sufficient for the practice's needs, you may connect to any network so long as the VPN is active and configured exactly as it was when the Security Officer approved it.

5. Online Services

What This Section Is About

This section is about those online services that Baltimore Therapy Center employs to keep our ship sailing. As a part of our team, you will make extensive use of these services, and you need to do your part in keeping client information secure when using them. This section describes the basic pieces of our policies that were adopted in order to maintain that security.

Security Policies Covered in This Section

This section covers essential information from the following security policies. You can find the current version of these policies in the workforce manual in your shared Google Drive.

- Bring Your Own Device Policy
- Information Systems Secure Use Policy
- Passwords and Other Digital Authentication Policy
- Facility/Office Network Security Policy

Using Your Personal Services

As described in the Bring Your Own Device Policy (and also the Business Associate Policy), you must only use services supplied by the practice to perform practice business. Using personal services would result

in PHI getting stored outside the practice's "circle," where the practice can't access the information and ensure that it stays secure.

Examples of personal services which you may not use for practice business include (but are not limited to):

- **Personal phone service, including voice calls, voicemail and texting. Be sure to only use phone and texting services supplied by the practice.**
- **Personal online "office" software. E.g. if you need to type up a letter or other document, use software supplied by the practice rather than using your personal Google Docs or Microsoft Cloud Office account. It may be permissible to use office software that stays on your device and doesn't use personal cloud services at all. Consult with the Security Officer if you are unsure.**
- **Personal secure texting or messaging services. E.g. even though Signal is a very secure app for texting, there isn't a way to keep it in the practice's "circle."**

Protecting your accounts on practice services

Baltimore Therapy Center employs services, e.g. Google Workspace, that are chosen for their practices of using good security measures and keeping client information safe. However, there are a few pieces of the security picture that only you can fill in.

The biggest piece is managing passwords and other forms of authentication. The Information Systems Secure Use Policy and the Passwords and Other Digital Authentication Policy include the following rules:

- USE STRONG PASSWORDS ONLY. See Rules for Strong Passwords and Other Forms of Authentication (below) for our definition of a "strong" password.
- KEEP PASSWORDS TO YOURSELF. Definitely do not share any of your passwords with others. *No member of the practice leadership will ever ask you to reveal any of your passwords*. As part of security auditing, a member of the risk management team may ask you if one or more of your passwords meets the practice's requirements for "strong" passwords (see Rules for Strong Passwords and Other Forms of Authentication below.) That is the limit of information that will ever be requested regarding your passwords, however. If you receive a request for password information beyond that, please report it to the Security Officer.
- PROTECT YOUR PASSWORDS. You need to keep your passwords secret from others.
- USE UNIQUE PASSWORDS FOR EVERY SERVICE. You need to ensure that the password you use for each of the Baltimore Therapy Center's services is unique and that you don't reuse any personal passwords. Password management software can help immensely to make this happen.
- USE 2-FACTOR AUTHENTICATION WHEN IT'S AVAILABLE. Two-factor authentication must be used for any systems where it is available.

The Information Systems Secure Use Policy also says:

- KEEP SERVICE ACCOUNTS TO YOURSELF. Don't share any of your service accounts with anyone else -- even if they are also permitted to use the service. Don't even share your account with someone

else “just for a few minutes.” One of the several reasons for this is: the Security Officer has a program of keeping track of how people are using our online systems, and it’s a pretty vital piece of our HIPAA compliance program. If you share logins or passwords, you may jeopardize our compliance process.

- DO NOT CHANGE SECURITY-RELATED SETTINGS ON SERVICES. Changes to configurations or settings in our online services are the purview of the Security Officer. Unless you’re taught or instructed otherwise, ask the Security Officer if you believe any settings or configurations should be changed.
- DO NOT SIGN UP FOR NEW SERVICES OR ADD NEW FEATURES TO EXISTING SERVICES. Ask the Security Officer if you believe new services are needed.

Keeping information “in the circle”

Certain services provide the ability to send or share information in ways that can cause client information to get outside the Baltimore Therapy Center’s “circle.” In general, you need to make sure you don’t do anything with a practice service that causes information to unintentionally get sent or shared outside of the service, unless the practice has created a specific procedure for doing that.

Here are some specific rules regarding keeping information inside our service systems that are spelled out in the Information Systems Secure Use Policy.

- **WITH EMAIL, TEXTING OR OTHER COMMUNICATION SERVICES, DO NOT FORWARD MESSAGES TO YOURSELF. We all have several different email accounts in our lives, and may even get texts or other communications from multiple sources. A common method of managing all these messages is to change their settings so that all your messages get forwarded to one central account. Unfortunately, setting up your accounts on practice services to do this would cause messages to leave the “circle,” and it would likely create confidentiality breaches, and possible availability loss. So don’t forward emails, texts, or other messages to yourself (or others.)**
- DO NOT SHARE FILES OR PROVIDE FILE ACCESS OUTSIDE OF THE PRACTICE. Some online services, e.g. Google Workspace, allow you to share access to files or other information with people outside of the practice. Unless you are following a procedure that has been established by the practice and approved by the Security Officer, do not use these sharing features to share information with accounts outside of those provided by the practice. E.g. do not share files with clients except where the practice has a procedure for doing that. Also, do not share access with your personal accounts or with a colleague’s personal account.

Record-keeping and other data entry for the practice’s online services

A big convenience offered by electronic record-keeping systems is the ability to enter and find information much more quickly than we can when working with paper. It also introduces some risks, however, that can create harm for clients or even cause confidentiality breaches. To reduce those risks, the Information Systems Secure Use Policy spells out the these rules:

- SESSION NOTES NEED TO BE CONSIDERED WITH FRESH EYES EACH TIME -- COPYING FROM OLD NOTES INTO NEW NOTES IS LIMITED. There is a large body of evidence that, when writing a session note, copying and pasting previously-created notes can cause important record-keeping errors. If notes are copied from a different client's record, there is also a risk of confidentiality breach.

  To prevent these errors, do not copy and paste anything between the records of multiple clients.

  It works to copy forward information within a client's record if it is the overall treatment plan or information about current progress (or lack thereof) towards goals. All other information needs to be written fresh. Do not copy and paste it from previous session notes. It does work, however, to use note-taking templates or data entry macros that contain no pre-filled information about the particular client.
- **WHEN ENTERING INFORMATION INTO AN ELECTRONIC SYSTEM; OR WHEN SENDING EMAILS, FAXES, OR OTHER COMMUNICATIONS THAT CONTAIN CLIENT INFORMATION; VERIFY THE RECIPIENT AT LEAST TWICE BEFORE TYPING/SENDING. Entering client info into the wrong record, and sending client info to the wrong person, are surprisingly common sources of small-yet-potentially-harmful confidentiality breaches.** So when you go to write a session note or enter client information in a system, double check that you are entering data into the correct person's record. When sending emails, faxes, etc. double check that you are sending to the correct person. Where possible, use contact book entries to help make sure your messages are going to the intended person.
- When scheduling online sessions in Google Meet, do not include the client as an invitee in your Google calendar. Instead, send them the Google Meet link to join at. This allows you to admit them rather than having them enter the meeting automatically.

Considerations on where you use practice services

As stated earlier, remember to be mindful of the context around you when using practice services

People behind you may be able to view your screen. Positioning your screen to avoid being viewed by others is not only a service to our clients and the practice, but it is also a service to the people around you.

When using the phone or video services, others may be able to hear you. Private spaces with sufficient sound dampening should always be used when on any type of call where clients or client information might be discussed.

Lastly, it is very important that you only use WiFi or other Internet connections that are trusted by the practice. Choosing Internet connections carefully is part of protecting the security of our online services. See the information about permitted WiFi and other connections under "WiFi and Other Internet Connections" above.

6. Communicating and Releasing Information

What This Section Is About

Electronic communication, especially texting, has revolutionized the way we engage with clients between sessions (or during sessions, if we're doing telehealth!) So, it's important to remember that our duty of confidentiality applies to any context where we engage with clients or their information. This section describes rules for maintaining client privacy and security when using electronic communications media to send client information.

Security Policies Covered in This Section

This section covers essential information from the following security policies. You can find the current version of these policies in the shared Security Policy folder.

- Communications Security Policy
- Release of Information Security Policy

How to communicate with clients (email, text, phone, etc.)

The Baltimore Therapy Center's default rule for communicating with clients is that only secure, Security Officer-approved services and media are used to communicate client information of any kind and for any purpose.

- Except where the client's safety is at stake, and there is no secure way to communicate something that is essential to their safety. In such a case, the client's safety should take precedence over the security of the communication method.

The following communications services/circumstances are considered *secure communications* that are in the Baltimore Therapy Center's "circle," and may be used to communicate client information without reservation (assuming the recipient of the information is permitted to receive it, of course.)

- Phone: Google voice, iPlum
- Email: Google Workspace/Microsoft 365
- Fax: not available
- Videoconferencing: Google Meet; County-provided Zoom & Microsoft Teams
- Texting: *secure* option not available

Release of Information Process

When releasing information about clients, whether it's just a letter or a whole client record, using a secure process is essential to maintaining clients' privacy.

Releases of information may look like any of these things, but this list is not exhaustive:

- Giving a client a copy of their health record; or giving it to a guardian of the client.
- Sending a letter about a client's treatment to a doctor's office, a case manager, a school counselor, a parole officer, or a variety of other professionals.

- Making a call regarding a client to other professionals, such as the ones listed above.
- Sending copies of client records to attorneys at the client's request.
- Release copies of client records to a court pursuant to a legal subpoena.
- Notifying a referral source about a client's compliance with treatment requirements.

The process by which information is released must satisfy these two areas of security:

- *Authorization* of the recipient. This means ensuring that the party receiving the information is allowed to view it.
- *Authentication* of the recipient. This means you've ensured that the party you are disclosing information to is, in fact, the party who was authorized to receive it.
    - E.g. if you are authorized to send a referral letter to the office of Dr. John Smith, make sure you have the right Dr. John Smith before sending!

When releasing information to other parties, the following needs to be done first in order to ensure that there is proper authorization to send it:

- Check the Release of Information (ROI) form associated with the release to ensure that it is signed by the right client or guardian, and that you are about to release the correct information based on the ROI.

Before releasing information, one or more the following needs to be done before sending it or handing it over:

- When speaking to someone on the phone whom you do not personally recognize, ask for the client's date of birth.
- When faxing or securely emailing documents, ensure that the phone/fax number or email address of the recipient matches what was written on the ROI.
- When handing documents to someone in person, if the person in question is not someone you recognize, you must require them to show ID to prove they are the person listed on the ROI.

In general, remember to take care that PHI being released to others is supposed to be released, and that it is being released to the proper party. If you are ever unsure, please consult the Security Officer *before* releasing anything.

Alternative communication process

The challenge behind a security-only setup is that clients and clinical staff often prefer communication by email or text message. Those media are, by convention, very poorly secured and we normally cannot use them to communicate any client information.

HIPAA allows (and so do the Baltimore Therapy Center's security policies), however, for clients to state that they wish to communicate with their clinicians and/or the practice staff using nonsecure means such as conventional email and SMS texting. In such a circumstance, the Communications Security Policy allows for certain nonsecure communications with clients under these conditions:

- The client has asked for nonsecure communications, such as conventional email or SMS texting, has requested nonsecure communications on the intake form and it is currently still valid and is on file with their record.
    - It is likely that any one of us can become part of the process when clients request to use nonsecure methods of communication. In such a case, you will be responsible for helping clients understand the risks to their privacy and, potentially, safety when making such a request. Ask the Security Officer for assistance in doing this if you do not have training or experience with it.
- The nonsecure communication medium (e.g. conventional email, SMS texting, etc.) you wish to use is permitted on the form that the client filled out, and the information you wish to send is also permitted on it.
- You are communicating *with the client* (or a guardian/caretaker with whom such coordination is permitted and appropriate), and not with someone else *about the client* (excepting the aforementioned guardian/caretaker, of course.)
    - Clients may specify in their Request for Nonsecure Communications that you may use nonsecure means to communicate with other parties. That should be a special case, however. Outside of particular special cases, your communication with collaterals should only be by approved, secure means.
- You are using one of the Security Officer-approved nonsecure methods described below.

The following communications services/circumstances may be used when the client has requested it and the process for using nonsecure communications has been completed:

- Email: If a client is having trouble accessing encrypted emails from us and they wish to receive unencrypted emails, emails from Office 365 are by default not encrypted; for Google Workspace you may enter the text "|nophi" into the subject line of an email to remove encryption.
- Texting: Google Voice or iPlum can be made available to you if needed.

7. The Security of Office Spaces

What This Section Is About

The Baltimore Therapy Center's office spaces are designed with the intention that some parts are open to anyone who comes by and has a reason to be there, and other parts are just for people involved in providing/receiving care, or in doing the Baltimore Therapy Center's business. We do a lot of sensitive things and keep a lot of sensitive information in those non-public areas, and we all need to do our part in keeping those sensitive things and information safe from security breaches. This section defines rules for accomplishing that.

Security Policies Covered in This Section

This section covers essential information from the following security policies. You can find the current version of these policies in the Security Policy folder.

- Facility/Office Access and Physical Security Policy

- Facility/Office Network Security Policy

Restricted and public areas

To help us organize the security of our spaces, the Facility/Office Access and Physical Security Policy defines these terms for different areas of practice offices:

- PUBLIC. Anyone may enter public areas.
- RESTRICTED: ESCORT ALLOWED. Anyone can enter escort-allowed areas if a member of the Baltimore Therapy Center's staff is with them. Note that if you are someone's escort, you don't have to shadow their every move. You simply need to be aware of where they are and act as the person who represents their reason for being in this area of the office.
- RESTRICTED: AUTHORIZED INDIVIDUALS ONLY. These areas are only for members of the staff.

Here is the breakdown of access permission for our offices:

1. Baltimore Therapy Center office
    - Public area: waiting room
    - Escort-allowed: back hallway, client meeting rooms
    - Authorized individuals only: none
2. Montgomery County office
    - Public area: main lobby
    - Escort-allowed: group rooms, staff offices
    - Authorized individuals only: all other areas

In the County building, people authorized to be in restricted-access areas should have a County badge.

Your part of maintaining the security of these spaces is simply to ask anyone who shouldn't be there to leave/return to the waiting room/lobby. If they are in an escort-allowed area, start by asking "who are you here to see?" If their clinician isn't "escorting" them, simply ask them to return to the waiting room/lobby.

If you discover someone where they shouldn't be, please do not put yourself at risk of harm or touch any such individuals in order to get them to leave the area.

When you discover such an individual, decide if it is safe to ask them to leave. If it does not appear to be safe, please seek appropriate help -- e.g., other workforce members, building security personnel, or police, as is warranted by the situation. You should never endanger yourself in order to remove an authorized individual from a restricted area. Please take care of you.

Securing sensitive equipment and documents

Any equipment or documents that handle sensitive information need to be kept in the possession of a staff member or inside a restricted area. If such equipment or documents are ever left without a staff member in the same room, they need to be locked up.

There are various, more specific rules for securing documents and devices described above. The general rule is that unattended equipment and documents need to be kept behind a lock when a staff member isn't there to monitor them.

Clinical Customer Document and Materials Protection Plan

Measure	**Location**	**Security Notes and Procedures**
Shredding physical PHI	*Client care rooms/staff offices*	*All physical PHI should be scanned and shredded immediately.*

Managing keys, badges, and door codes

Many parts of our offices are protected by locks. As you work with the Baltimore Therapy Center, you may be issued various keys and codes for opening doors and possibly other things with locks on them.

When you have been issued a key or access code, it is important that you keep it to yourself and not share it with others. Also, do not make copies of keys. If you need multiple copies of a key, ask the Security Officer about it rather than making your own copies.

If a colleague at the Baltimore Therapy Center is authorized to be in a space for which they don't possess a key or access code, feel free to let them in with your key or access code. Do not, however, share with them your key or tell them the code. If they need either item, they need to inquire with the Security Officer rather than with you.

Handling PHI in Public Areas and Away from the Office

Sometimes you need to handle PHI in a public place, such as in the practice's public spaces or while away from the office. Here are some examples of such times, although the list is not exhaustive:

- Processing intake forms at a desk in the waiting room
- Talking to clients in the waiting room
- Talking to or about clients on the phone while at home or out and about
- Discussing client cases with colleagues away from the practice's private spaces
- Working on session documentation while in a semi-public or public space

When handling PHI in public, you need to:

- Take conversations and phone calls away from other people (including family or others you normally trust with private information.) If you can't find a fully private spot, ask to finish the conversation another time. If you must continue the conversation, quiet your voice and use anything you can to muffle the sound from others.

- If working on a computer or on documents, sit so that other people cannot stand or sit behind you. For example, sit with your back to a wall. If you have a polarizing screen cover for your computer, please use it.
- If anyone wishes to speak with you while you are working with practice documents on paper or a screen, ask them to wait a moment. Then hide the contents of the paper or device away before initiating any conversation with them.

In general, it is of great importance that you take steps to maintain the privacy of client information regardless of where you are while you handle it.

WiFi and other Internet access

Office spaces used by the Baltimore Therapy Center will have Internet connections available for the staff and may also have connections available for clients and other visitors.

Internet connections, such as WiFi networks, will always be separated so that the staff use a different network than clients and other visitors use. So when you have the staff WiFi password, you need to keep it to yourself. If there are other Internet connections in the office, such as physical ports that can be plugged into, only staff may use them.

Staff and guest Internet networks at the Baltimore Therapy Center break down like this:

- Baltimore Therapy Center office
    - Public Internet: BTC-guest (password: thingscanbedifferent)
    - Staff-only Internet: BTC-5G

Backup Internet Connections

Because it is imperative that everyone have Internet access in order to perform their jobs, we have defined the following options for acquiring and using backup Internet access. These methods of access may be used any time that practice-provided Internet access is unavailable for any reason.

- Personal cellular data connections, such as on your smartphone. Do not share your smartphone hotspot with others while using it.
- Any Internet connection may be used so long as you have an active VPN protecting your device for the entire time that it is connected. Your VPN service must have a “kill switch” activated to ensure that your devices do not lose VPN protection unexpectedly.

Securing Remote Workspaces

If you perform practice work from a remote workspace, including a home office, it is important to ensure you have proper security measures in place. Ensure all the security behaviors outlined in this chapter of the manual are implemented in your remote workspace.

8. Security Incidents

What This Section Is About

We do a lot at the Baltimore Therapy Center to prevent security issues, but we also need to be ready to respond when security issues do arise. This section defines rules for helping the Baltimore Therapy Center "detect" and respond to such incidents.

Security Policies Covered in This Section

This section covers essential information from the following security policies. You can find the current version of these policies in the Security Policy folder.

- Security Incident Response and Breach Notification Policy

How to report an incident

When you discover an incident, please complete an Incident Response Form and submit it to the Security Officer. The Security Officer or a member of the incident response team may need to ask you follow up questions about what you discovered. Please be available to help the team investigate the incident.

How to recognize an "incident"

Importantly, a security *incident* is not the same thing as a security *breach*. Determining if an actual breach occurred will be the job of the Security Officer and anyone they team up with to investigate an incident. Your job is simply to help the Baltimore Therapy Center and the Security Officer to recognize when potential breaches have occurred and to report them.

Some portions of this manual instruct you to make a security incident report in certain circumstances. We cannot anticipate all the possible situations that merit a report, however. So here is the general rule for when you should make a report to the Security Officer about a security incident:

If anything occurs that looks as if there may have been an inappropriate disclosure of client information, or if it appears that someone may have used client information inappropriately, or it seems that an opportunity for either of those things to occur has arisen, please report it. Also, please report any incident that indicates that client information may have been inappropriately edited, damaged, or lost.

You are not expected to differentiate between actual breaches or risks of breach and incidents which simply look like breaches or risks of breach. You can simply report and let the Security Officer and their team figure it out.

9. Rules for Strong Passwords and Other Forms of Authentication

What This Section Is About

Passwords, 2-factor authentication, and the like are a big deal in a practice that uses a lot of electronic services and systems. This section will help lay out the rules for making sure your authentication practices are effective and meet Baltimore Therapy Center's needs.

Security Policies Covered in This Section

This section covers essential information from the following security policies. You can find the current version of these policies in the workforce manual in your shared Google Drive.

- Passwords and Other Digital Authentication Policy

Passwords and Other Authentication Rules

The Baltimore Therapy Center requires that workforce members comply with the following password and authentication requirements:

- Strong passwords are required
    - A strong password is defined as any of the following:
        1. A password that is at least 12 characters in length and contains at least one capital letter, one lowercase letter, one number, and one punctuation character.
        2. A passphrase that is at least 4 words in length, where the words have no logical relationship with each other.
        3. A passphrase made up of a sentence, but with at least 5 words and at least one number and one punctuation character.
- **Passwords must be unique. The same password must not be used for multiple accounts or devices.**
- Passwords must be changed on at least a semi-annual basis.
- Multi-factor authentication is required.
    - If 2-factor authentication is available, it must be used.
    - If 2-factor authentication is not available then the service in question may be used without it.
- The use of a Password Management Program is recommended.
- **Passwords may not be written down.**

10. Emergency Mode Operation Plans

What This Section Is About

Things don't always go as expected, and that is why the practice has developed the following contingency plans for helping us respond to emergencies as orderly and effectively as we can.

Every workforce member needs to read the following plans and have a general idea of:

- When it will be time to execute the plan.
- What your role will be in executing the plan.

Security Policies Covered in This Section

This section covers essential information from the following security policies. You can find the current version of these policies in the Security Policy folder.

- Contingency Planning Policy

Contingency Plan

The following operations must be performed despite interruptions:

- Providing treatment sessions to clients
- Communicating about administrative matters with clients/guardians

If clinical services cannot be delivered at the office, staff will attempt to reschedule to telehealth and clinical staff will prepare for telehealth sessions according to the practice's policies regarding that delivery medium. Clients who refuse telehealth sessions will be rescheduled for a time that is presumably after normal operations resume.

If telehealth services are inaccessible, staff will contact clients to inform them that services are unavailable and will resume when telehealth platforms are accessible again.

If the practice management system becomes unavailable, keep notes on a secured device until they can be uploaded to the cloud system.