General Privacy Policy

Be Well Clinic (The Practice) is committed to protecting the privacy of its Patients, and is required by applicable federal and state laws and regulations to maintain the privacy of Patients' protected health information (PHI). The primary elements of the Practice's privacy policy include, but are not limited to, the following:

1. The Practice designates Owner as the Privacy and Security Officer for the Practice.

2. The Practice will publish a notice of privacy practices (Notice) and post the Notice in a clear and prominent location in the Practice. The Practice will provide the Notice to new Patients at their initial visit to the Practice. Copies of the Notice will be available to any individual upon request.

3. The Practice will make a good faith effort to obtain Patients' written acknowledgment of receipt of the Notice. If unable to do so, the Practice will document its efforts to obtain the written acknowledgment, as well as the reasons why it was unable to do so.

4. All workforce members of the Practice will at all times limit, to the minimum extent necessary, access to, and the use and disclosure of, PHI.

5. The Practice will use a valid HIPAA authorization form to obtain written authorization for uses and disclosures of PHI for purposes other than treatment, payment, or as otherwise permitted or required by law and HIPAA regulations. The Practice will retain all signed HIPAA authorization forms for a period of at least 10 years.

6. The Practice will investigate all reported violations of any privacy policy and will develop and implement a plan of action to correct violations.

7. The Practice will provide introductory training to all employees and contractors regarding privacy rules and regulations, as well as the Practice's privacy policies and procedures. The Practice will also offer periodic refresher training.

8. The Practice will require all employees and contractors to take the Post HIPAA Education Quiz and results of 80% or higher. If the results fall under 80%, additional training will be required.

9. The Practice will maintain documentation of its compliance with HIPAA for Federal Register Guidelines.

Privacy Officer

The Privacy Officer for the Practice is Amy Mihaly.

The Privacy Officer is responsible for overseeing HIPAA compliance and implementation of the Practice's privacy policies, procedures, and training. The Privacy Officer is responsible for updating and changing Practice policies as necessary or as required by law.

Specifically, the Privacy Officer is responsible for:

1. Developing HIPAA compliance policies, procedures and standards.

2. Overseeing and monitoring implementation of HIPAA compliance.

3. Revising HIPAA-related policies, procedures and forms to reflect changes within the Practice, changes in the law or in governmental rules and regulations.

4. Ensuring that all employees and contractors receive HIPAA training, including related policies and procedures regarding the handling of PHI. Workforce members will be trained upon joining the Practice and will obtain additional training when there is a material change to the Practice's policies or procedures.

5. Developing, coordinating, and/or conducting educational activities and communications focusing on HIPAA-related compliance activities. Educational activities may include training seminars and dissemination of educational materials and updates to employees and contractors.

6. Ensure that all relevant workforce members, providers, consultants and contractors comply with HIPAA and other relevant federal and state laws, rules, and regulations regarding privacy of Patient information.

7. Conducting or assisting with internal HIPAA compliance reviews and audits, as warranted.

8. Ensuring that employees and contractors know that they can report suspected violations and other improprieties without fear of retaliation and that they are encouraged to do so.

9. Investigating HIPAA-related compliance issues and bringing them to the attention of necessary personnel or authorities for appropriate response.

10. Serving as the point person for HIPAA-related concerns or complaints about the Practice and the handling of all Patient Rights' requests.

11. Maintaining complete and accurate documentation of the Practice's compliance with HIPAA.

General Information Safeguards

The Practice is required by the Health Insurance Portability and Accountability Act (HIPAA) to have in place appropriate administrative, technical, and physical safeguards to protect the privacy of our Patient's Protected Health Information (PHI). The Practice is also required to reasonably safeguard PHI from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of HIPAA.

The Practice is committed to reasonably safeguarding our Patients' PHI to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

Examples of safeguards utilized by the Practice to protect Patients' PHI include:

1. All documents containing PHI are to be shredded prior to disposal by the Practice.
2. Areas within the Practice containing Patient PHI shall be locked when not in use.
3. File cabinets containing Patients' medical records are to be locked at the close of the business day.
4. During the day, Patient records are to be stored in such a manner that Patient guests and family members are unlikely to see the Patient's PHI.
5. Only authorized personnel will have access to the Practice during non-regular business hours.
6. The Practice will remove electronic information system access containing PHI and passwords will be changed.
7. Providers' and workforce members' access to PHI via the Internet or phone modem shall be appropriately authenticated and protected.

Identifying Patient Health Information

The following information will be designated as PHI:

Any health information, including demographic information, collected from an individual, transmitted, or maintained in any form or medium, that: a) is created or received by the Practice; b) relates to (i) the past, present or future physical or mental health or condition of an individual, (ii) the provision of healthcare to an individual, or (ii) the past, present or future payment for the provision of healthcare to an individual; and (c) identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

1. Routine health information meeting the above definition will automatically be designated as PHI immediately upon its creation or receipt by the Practice.
2. The Practice will adhere to all applicable laws, regulations, policies and procedures when maintaining, using and disclosing Patient PHI.
3. Appropriate steps will be taken to properly identify and secure individuals' PHI. In the event of a discrepancy as to what constitutes PHI, the Privacy Officer will be consulted for guidance and recommendations.

Allowable Uses and Disclosures of PHI

The Practice may, without an Authorization, use or disclose PHI to the Patient, or for treatment, or payment, as defined in HIPAA. The Practice may also disclose information to a Patient's family member, other relative or close personal friend, but only that information directly relevant to the person's involvement in the Patient's care, payment, or for notification purposes. This provision also applies when the Patient is not present, is incapacitated, or is in an emergency situation, or if the family member, other relative or close personal friend was involved in the Patient's care or payment for care prior to the Patient's death.

Under HIPAA's Privacy Rule, the Practice is also permitted to disclose PHI without an Authorization if federal, state and/or local laws require the disclosure. In that case, the Practice may disclose only to the extent that the disclosure complies with, and is limited to the requirements of, the law.

The Practice may disclose a Patient's PHI to government authorities (including a social services or protective services agency) authorized by law to receive such reports, if the Practice reasonably believes the Patient to be a victim of abuse, neglect or domestic violence.

The Practice may disclose PHI to a health oversight agency for oversight activities authorized by law, including audits, investigations, inspections, licensure or disciplinary actions and proceedings.

The Practice will comply with all lawful and appropriate requests from regulatory and judicial authorities and disclose PHI necessary to respond to a valid subpoena, discovery request or other lawful process. [The Practice will only disclose that PHI the Patient has expressly authorized be disclosed]. Any employee or contract worker member receiving a subpoena for Patient records is encouraged to forward it to the Privacy Officer for review and approval prior to processing the request.

Members of law enforcement who request medical information in the absence of proper documentation should be referred to the Privacy Officer before the release of any PHI.

The Practice may, consistent with all applicable laws, disclose PHI if it believes in good faith that the disclosure is necessary to prevent or diminish a serious and imminent threat to the health or safety of a person or the public.

The Practice may disclose PHI to coroners, medical examiners and funeral directors in order for them to carry out their professional duties. Information may also be given to

organ procurement organizations for the purpose of facilitating organ, eye or tissue donation and transplantation.

The Practice may disclose PHI as authorized by, and to the extent necessary to comply with, laws related to workers' compensation or other similar programs established by law that provide benefits for work-related injuries or illness without regard to fault.

Confidentiality, Integrity and Availability of Electronic PHI

HIPAA specifies 3 types of safeguards for protecting PHI maintained in electronic formats: administrative, physical and technical.

1. Administrative safeguards include administrative actions processes and policies and procedures that manage (a) the selection, development, implementation, and maintenance of security measures to protect PHI and (b) the conduct of the Practice's workforce in relation to protecting that information.

2. Physical safeguards are the mechanisms required to protect electronic systems, equipment, and their data from threats, environmental hazards and unauthorized intrusion. They include restricting access to PHI, retaining off-site computer backups, workstation security, and data backup and storage.

3. Technical safeguards are primarily the automated processes used to protect and control access to electronic PHI. They include using authentication controls to verify that a person signing onto a computer is authorized to access PHI, encryption, and mechanisms to protect data from unauthorized alteration or destruction.

Social Media

The Practice recognizes that participating in social networking and other similar Internet opportunities can support workforce members' personal expression, enable Providers to have a professional presence online, foster collegiality and camaraderie within the profession, and provide an opportunity to widely disseminate public health messages and other health communication. However, social networks, blogs, and other forms of communication online also create new challenges to the privacy and confidentiality of Patient PHI.

1. The Practice encourages all workforce members and Providers to be cognizant of standards of Patient privacy and confidentiality that must be maintained in all environments, including online, and must refrain from posting identifiable Patient information online.

2. When using the Internet for social networking, workforce members and Providers should use privacy settings to safeguard personal information and content to the extent possible, but should realize that privacy settings are not absolute and that once on the Internet, content is likely there permanently.

3. Providers who interact with Patients on the Internet must maintain Patient/Physician relationship boundaries in accordance with professional ethical guidelines.

Personal Representatives

As required by HIPAA, if the Patient has designated an individual to act on his or her behalf, or if state or other law has determined that an individual is authorized to act on behalf of a Patient (Personal Representative), the Practice will treat the Personal Representative as the individual for purposes of HIPAA. This includes the right of access to the Patient's PHI in accordance with HIPAA regulations.

The scope of a Personal Representative's access will depend on the authority granted to him/her by law. For example, if a Personal Representative's authority is limited to authorizing artificial life support, then the Personal Representative's access to the Patient's PHI will be limited to information relevant to decisions about artificial life support.

The Practice of BeWellClinic, LLC will identify Personal Representatives of Patients in the following manner:

The Practice will request any necessary written documentation or administrative order verifying the Personal Representative's authority to act on behalf of the Patient regarding the disclosure of PHI, for example, maintaining a copy of the Patient's valid Durable Medical Power of Attorney in the Patient's file.

1. In the case of minors, documentation will only be required if the requestor is not known to the Practice. It will be assumed that parents are the Personal Representatives of their minor children *unless* there is a reason for the Practice to believe otherwise.

2. If the Practice is unable to obtain adequate documentation of an individual's Personal Representative status, the Practice may use professional judgment in using or making a disclosure of PHI to a Patient's family member, other relative, or close personal friend if such individual is involved in the Patient's care and/or payment related to the Patient's care, for notification purposes, and in emergency situations.
3. The Practice may also use its professional judgment and experience with common practice to allow a relative or close personal friend of the Patient to pick up the Patient's prescriptions, medical supplies, or other forms of PHI.
4. The Practice retains the right not to disclose PHI to a Personal Representative, if, in the exercise of its professional judgment, the Practice believes that disclosing the PHI would not be in the best interests of the Patient because the Practice reasonably believes the

Patient has been, or may be, subject to domestic violence, abuse or neglect by the Personal Representative, or that disclosure would otherwise endanger the Patient

Training in Privacy and Security

The Practice of BeWellClinic, LLC recognizes that training in privacy and security is essential to the Practice's HIPAA compliance program.

1. All new Practice workforce members will complete general HIPAA training within 30 days of hire. Workforce members will sign the Workforce Member Acknowledgement of Training certifying they have taken the training and understand HIPAA compliance and the Practice's policies and procedures related to HIPAA compliance implementation.

2. All new workforce members who have access to electronic systems containing PHI will complete HIPAA privacy and security training as soon as possible after gaining access to the systems. Preferably, security training will occur prior to initiating access to systems containing PHI.

3. Existing workforce members will take annual refresher training on HIPAA privacy and security. Workforce members who are out of compliance with this standard face possible revocation of their access rights to systems containing electronic PHI, and will be referred to the Privacy Officer for consideration of administrative actions and further sanctions.

4. The Practice will review, and revise if necessary, its HIPAA training courses on a routine basis. Newly identified risks to the Practice will be incorporated into the Practice's training programs as they are identified.

5. The Practice will document all training of its workforce and will maintain this documentation for a period of 6 years.

Questions about HIPAA training should be directed to the Privacy Officer.

Breach Notification Process

A breach of PHI shall be treated as "discovered" as of the first day on which the Practice knows of the breach, or would have known of the breach by exercising reasonable diligence.

Therefore, it is crucial that all workforce members remain on high alert for potential or suspected breaches, and notify the Practice's Privacy Officer immediately (in no case later than 24 hours after discovery of the breach). This allows the Practice to take appropriate steps to mitigate, investigate and notify in a timely manner.

Timeliness of Notification

Timeliness of notification is critical. Therefore, the Practice will send written Notice of the breach to the affected Patients and other entities as promptly as is reasonably possible after completing its investigation of the breach, but without unreasonable delay, and in no case later than 60 calendar days after the Practice discovers the breach.

Content of Notification

An affected Patient will receive written Notice of a breach of his/her unsecured PHI by first class mail to the last known address of the Patient. (If the Patient has agreed to receive information from the Practice electronically, i.e. via email, then the Notice may be sent electronically instead of via first class mail, unless the Patient has withdrawn his/her agreement.)

The written Notice will include the following elements:

1. A brief description of what happened;
2. The date of the breach and the date the Practice discovered the breach;
3. A description of the type of unsecured PHI that was involved in the breach (e.g. social security numbers, diagnoses information, address, date of birth, etc.);
4. Steps Patients should take to protect themselves from potential harm as a result of the breach;
5. The Practice's apology that the breach occurred;
6. A brief description of what the Practice is doing to investigate, mitigate, and protect against further breaches; and

The Notice will be written as simply as possible using clear and understandable language and at an appropriate reading level for the Practice's Patients.

Special Situations

1. In urgent situations where the Practice determines it should notify a Patient of the breach of his/her unsecured PHI prior to concluding its investigation, the Practice may call or otherwise contact the Patient to inform him/her of the breach. However, the Practice will also send written Notice to the Patient/s within the timeframe required by the Rule.

2. When a minor child's unsecured PHI is breached, the Practice will send the Notice to the child's parents/guardians.

3. If a deceased Patient's PHI is breached, Notice will be sent to the Patient's next of kin or personal representative, if known to the Practice. If the Practice does not have information for a deceased Patient's next of kin or personal representative, Notice for the deceased Patient need not be sent.

Substitute Notice

If the Practice does not have sufficient contact information for more than 10 Patients whose unsecured PHI was breached, the information contained in the written Notice will be posted on the home page of the Practice's website for 90 days.

Methods of Notification

The Privacy Officer will be the key facilitator for all breach Notifications to appropriate parties (e.g., affected Patients, HHS, media outlets, law enforcement officials (if necessary).

The Practice will maintain a log of breaches involving any individuals and will provide notification within 60 days after the end of the calendar year in which the breaches were discovered.

The Practice will consider offering credit monitoring services to individuals affected by a breach when sensitive identifiers such as social security numbers and credit card account information are lost or inappropriately accessed, used or disclosed. The Privacy Officer will make the initial determination as to whether or not to consider offering this protection to affected Patients.

Law Enforcement Delay

The Practice will delay providing Notice of a breach if a law enforcement official determines that Notification would impede a criminal investigation or damage national security. If the Practice receives a verbal request from law enforcement to delay Notification, the Practice will delay Notification for up to 30 days. If a law enforcement official determines that more time is necessary, he/she must submit a written statement to the Practice, detailing the specific timeframe for delay.

Business Associates' Responsibilities

The Practice's Business Associates will be required to notify the Practice of any breach or potential breach of PHI, including the identity of each Patient whose PHI is believed to have been breached, in a timely manner (in no case longer than 7 days after discovery) in order to allow the Practice to provide required Notifications as soon as possible. Business Associates are also required to ensure that any Subcontractor Business Associate that breaches the Practice's Patients' PHI notify the Business Associate in a timely manner (in no case longer than 7 days after discovery of the breach) who, in turn, will notify the Practice.

Documentation

In accordance with the requirements of the Breach Rule, the Practice will record and log all breaches of unsecured PHI, regardless of the number of Patients affected.

The Practice will also thoroughly document all potential breaches determined, after performing a risk assessment, to pose only a low probability of risk (for which individuals, HHS and the media (if applicable) are not notified of the incident).

All documentation will be maintained by the Practice in written form (paper or electronic) for a period of at least 10 years.

Sanctions

The Practice of BeWellClinic, LLC will take appropriate disciplinary action against any workforce member or Provider who violates its privacy and security policies and procedures or local, state, or federal privacy laws or regulations, including the HIPAA Rules.

Failure to comply with the Practice's privacy policies or procedures will result in disciplinary action. The Practice will enforce sanctions consistently.

Disciplinary action will be determined on a case by case basis, taking into consideration the specific circumstances and severity of the violation. Sanctions that may be imposed include, but are not limited to:

a. a verbal warning;
b. a letter to the workforce member's or provider's personnel file;
c. removal of system privileges;
d. administrative leave without pay;
e. attendance and successful completion of additional privacy training; or
f. termination of employment.
g. Violations of HIPAA may also result in civil and/or criminal penalties for workforce members and Providers imposed by local, state and federal authorities.

Any workforce member who observes, becomes aware of, or suspects a wrongful use or disclosure of PHI maintained by the Practice is required to report the incident to the Practice's Privacy Officer as soon as possible.

The Practice will not retaliate against any workforce member who makes a good faith report of a suspected or actual improper use or disclosure of PHI.

A workforce member's failure to report a suspected or actual violation of HIPAA is a violation of the Practice's policies and procedures. Such failure to report may subject the workforce member to disciplinary action, up to, and including, termination.

Open Door Policy

The Practice maintains an Open Door Policy regarding HIPAA compliance. All workforce members are encouraged to speak with the Privacy Officer regarding any concern they may have with the Practice's HIPAA compliance program or initiatives designed to maintain the privacy and security of PHI. As such:

1. HIPAA compliance will be discussed periodically at staff meetings to ensure understanding of all policies and procedures.

2. Informal methods of communication may also be used to communicate privacy and security compliance issues. This may include use of the Practice's office bulletin board for important updates or email communications.

3. Workforce members will be periodically reminded that failure to report fraudulent or erroneous conduct regarding privacy or security issues is considered a violation of the Practice's HIPAA compliance program and that there will be no retribution for the reporting of activities that a reasonable person acting in good faith would believe to be fraudulent or erroneous. (See Non-Retaliation Policy)

4. Whenever possible, anonymity will be maintained in connection with reports; however, the Practice cannot ensure anonymity in all cases.

Non-Retaliation Policy

All workforce members of the Practice BeWellClinic, LLC will refrain from intimidating, threatening, coercing, discriminating against, or taking any other retaliatory action against any workforce member, Patient, family member, or other individual for exercising any right under, or for any process permitted or required by, the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The Practice is committed to protecting Patient privacy as mandated by state, federal and other laws, and encourages its workforce members and affiliates to report actual or suspected violations of privacy laws and regulations without fear of retaliation.

The Practice will not retaliate against any workforce member, Patient, or other individual for:

1. exercising any right granted under, or participating in any process established by, state, federal or other privacy laws and regulations, including those rights and processes mandated in HIPAA; or

2. filing a complaint with the Practice about an improper or unauthorized use or disclosure of a Patient's PHI; or

3. testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing related to HIPAA; or

4. opposing, in good faith, any act or practice made unlawful by privacy laws, regulations, or policy (as long as the manner of the opposition is reasonable and does not use or disclose PHI in violation of HIPAA); or

5. making a good faith report of a suspected or actual improper use or disclosure of PHI.

The Practice maintains an Open Door Policy that encourages workforce members to report actual or suspected problems and concerns. Any workforce member who observes, becomes aware of, or suspects a wrongful use or disclosure of PHI maintained by the Practice is required to report it as soon as possible to the Practice's Privacy Officer.

Any workforce member who commits or condones any form of retaliation will be subject to discipline up to, and including, termination.

Business Associates

The Practice may disclose PHI to a Business Associate and allow a Business Associate to create or receive PHI on its behalf, if it obtains satisfactory assurances of compliance by entering into a written Agreement with the Business Associate (Business Associate Agreement or BAA) that establishes the permitted and required uses and disclosures of PHI.

The Practice will ensure that Business Associate Agreements or Contracts between the Practice and its Business Associates comply with the HIPAA Rules.

This includes a requirement that the Business Associate report to the Covered Entity (i.e., the Practice) any incident of which it becomes aware, including breaches of unsecured PHI, as required by the HIPAA Rules.

A Business Associate of the Practice will ensure that any Subcontractors that create, receive, maintain or transmit PHI on behalf of the Business Associate agree to comply with the HIPAA Rules by entering into a written Agreement with the Business Associate that establishes the permitted and required uses and disclosures of PHI.

> *If the Practice learns that a pattern of activity or practice by a Business Associate constitutes a material breach or violation of the Business Associate's obligation under its BAA or Contract, the Practice will take reasonable steps to cure the breach or end the violation. If such steps are unsuccessful, the Practice will terminate the Contract with the Business Associate, if feasible.*

Workforce Member Hiring and Termination Procedures

The Practice has established the following policies and procedures regarding the hiring and termination of its workforce members:

1. The Practice will check a minimum of 2 references for each potential workforce member being considered for employment.

2. The Practice reserves the right to conduct credit reports and/or criminal record checks on potential workforce members.

3. During exit interviews with workforce members whose employment with the Practice is terminated, the Practice will attempt to learn if the workforce member had privacy/security concerns that he/she was uncomfortable reporting to his/her supervisor.

4. Each exiting workforce member will be reminded of his/her continued confidentiality obligations regarding the Practice's PHI.