Date:_____ Position Applied For:_____

Application for Employment

We are an equal opportunity employer and do not unlawfully discriminate in employment. No question on this application is used for the purpose of limiting or excluding any applicant from consideration for employment on a basis prohibited by local state or federal law. Equal access to employment, services and programs is available to all persons. Those applicants requiring reasonable accommodation to the application and or interview process should notify a representative of the organization.

Name:_____ Social Security Number:_____ DOB:_____

Address:_____Town:_____ZIP:_____

Cell phone#:_____ Home #_____ Email:_____

Date you can start work:_____Hours per week DESIRED:_____

Hours Available to Work:

Monday	Tuesday	Wednesday	Thursday	Friday

I hereby authorize the potential employer to contact, obtain and verify the accuracy\\cy of \information contained in this application from al previous employers educational institutions and references. I also hereby release from \liability the employer and its representatives for seeking gathering and using such information to make employment decision and all other persons or organizations for providing such information.

I understand that any misrepresentation or material omission made by me on this application will be enough cause for cancellation of this application or immediate termination of employment if I am employed, whenever it may be discovered.

If I am employed, I acknowledge that there is no specified length of employment and that this application does not constitute an agreement or contract for employment. Accordingly, either I or the employer can terminate the relationship at will, with or without cause, at any time, so long as there is no violation of applicable federal or state law.

I understand that it is the policy of this organization not to refuse to hire or otherwise discriminate against a qualified individual with a disability because of that persons need for a reasonable accommodation as required by the ADA.

I also understand that if I am employed, I will be required to provide satisfactory proof of identity and legal work authorization within 3 days of being hired. Failure to submit such proof within the required time shall result in immediate termination of employment.

I represent and warrant that I have read and fully understand the foregoing, and that I seek employment under these conditions.

Applicant Signature:_____Date:_____

Payroll Policy

The payroll period starts on Monday and end on Saturday. Each paycheck is for a 2-week period. The official pay date for the 2-week period\s\d is the Friday following the Saturday which ends the 2-week period. If the office is closed on that Friday, the paychecks will be distributed on the following Monday.

In the event you are receiving your final paycheck and you were issued keys, you keys must be returned prior to the Friday when paychecks are handed out

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
1	2 **Pay period starts**	3	4	5	6	7
8	9	10	11	12	13	14 **Pay Period ends**
15	16	17	18	19	20 **Pay checks Distributed**	21
22	23	24	25	26	27	28

Dress Policy

It is our responsibility to project an image of professional health care providers to our patients, their family members as well as our referring physicians who have entrusted us to treat their patients. Our dress, behaviors and attitudes convey a message to our patients; especially on their first visit to our office. First impressions are hard to break. It is with these in mid that we have instituted our dress policy:

Dress Code: No sweat pants, sandals, or open toed shoes. No shorts, skirts are allowed during the summer and must come to the knee. Clothing must be clean and free of offensive odors. Jeans with deigned rips, cuts or holes are not allowed. Clothing with printed messages political, religious or otherwise are forbidden. Slacks such as Dockers and polo shirts are great. There will be no wearing of jewelry in facial piercings while working (except earrings which are fine) The office manager or other designated supervisor may use their sole discretion as to the what is or not appropriate.

Signature:_____Date:_____

Attendance Policy

1. If you are sick DO NOT COME TO WORK.
2. If sick, You MUST call, text or email (trohrs123@yahoo.com), the office (718) 945-9575, office manager (516) 965-7740 or owner PRIOR to the start of your shift.
    a. If you do not contact us prior to the start of your shift it is grounds for immediate termination.
3. One day out sick does NOT require a doctor's note. IF, you call out sick for a 2nd day, a doctor's note or note from emergency room is required to clear you to return to work. IF you do not bring in note clearing you to work, that you have recovered from your illness, YOU CANNOT RETURN TO WORK.
4. All employees must be on time for work. When you punch in for work you should be dressed and ready for work. It is unacceptable to punch in for work then take off your snow boots, change your shoes, eat your breakfast etc.
5. All employees must come back from lunch on time.
6. You must request time off 2 full weeks in advance of the day /days you need off.

Signature: _____Date:_____

Cell Phone Policy

Our cell phone policy has been designed to ensure that our staff acts in a professional manner, focusing our sole attention on our number job: patient satisfaction. It is imperative that patients receive the best care possible as well as having a mistake free experience at our reception desk. In the gym, patients must always be monitored to ensure that they are performing exercises safely and correctly, that we are watching for abnormal responses to exercise and to move them along efficiently in their program.

To that end our policy:

All employees, physical therapists, physical therapist assistants, aides, billers and receptionists will place their cell phone in the lock box before they punch in. Upon punching out for lunch you may retrieve your cell phone. Again, as you return from lunch you are required to place cell phone in lock box and it will be returned to you upon punching out for the day.

1st Violation: Written warning

2nd Violation: Termination

Internet Wi-Fi Policy

To ensure that we are following all HIPAA privacy protection laws, no employee is to connect their personal cell phone tablet or any other device to the Wi-Fi network. In addition, no employee shall give the wi-fi password to any patients, vendors, repair people or landlord except for Charmaine from Sky Technology our IT company.

It is against company policy for any employee to use company computers and internet for non-work-related web surfing. That means no You Tube videos, online shopping etc.

1st Violation: Written warning

2nd Violation: Termination

Eating and Drinking

It is against company policy to be eating or drinking in front of patients. There is to be no eating or drinking at the reception desk or in the gym. The kitchen is the only acceptable place to eat or drink.

1st Violation: Written warning

2nd Violation: Termination

Signature: _____Date:_____

Job Duties

As an employee of Sands Point Physical Therapy it is you duty to perform those tasks necessary as instructed by the owner office manager of person designated as supervisor by owner. You job title may be "Receptionist" or "PT Aide", but everyone is responsible to perform any task assigned by management team.

It is unacceptable to say, "That is not my job". If instructed to perform a task and you refuse and reply that it is not you job it is grounds for immediate termination.

Signature:_____Date:_____

Discipline

It is at the sole discretion of management to decide how individual employees will be disciplined for company policy infractions. Some may receive a written or verbal warning; while others may be terminated immediately.

I have the read above stated policies and understand them and agree to abide by the guidelines set forth.

Employee Name:_____Employee Signature:_____Date:_____

For Office use only

Reviewed by:_____ Starting salary:_____Start Date:_____

Sands Point Physical Therapy

Confidentially and Non-Disclosure Agreement

Organizational information that may include, but not limited to, financial, patient identifiable, employee identifiable, intellectual property, financially nonpublic, contractual or competitive advantage nature, and from any source or in any form (I.E. paper magnetic or optical media digital conversations film etc.) may be considered confidential. Information's confidentiality and integrity are to be preserved and its availability maintained. The value and sensitivity of information is protected by law and by the strict policies of Sands Point Physical Therapy. The intent of these laws and policies is to assure that confidential information will remain confidential through its uses, only as a necessity to accomplish Sands Point Physical Therapy mission.

As a condition to receiving a computer Log on Code and allowed access to a computer system, and/or being granted authorization to access any form of confidentially information identifies, I the undersigned agree to comply with the following terms and conditions:

1. My Log On Code, is equivalent to my LEGAL SIGNATURE and I will not disclose this code to anyone or allow anyone to access the system using my LOGN ON Code.
2. I am responsible and accountable for all entries made and all retrievals accessed under my Lon On code, even of such action was made by me or by another due to my intentional or negligent act of omission. Any data available to me will be treated as confidential information.
3. I will not attempt to learn or use another Log On Code
4. I will not access any on-line computer system using a Log On Code other than my own.
5. I will not access or request any information I have no responsibilities for. In addition, I will not access any other confidential information, including personal, billing or private information.
6. If I have any reason to believe that the confidentiality of my Log On Code/password has been compromised, I will immediately change my password and notify Sandy Rohrs and or Timothy Rohrs, PT, DPT.
7. I will not disclose any continental information unless it is required to so so in the official capacity of my employment or contract. I also understand that I have no right or ownership interest in any confidential information.
8. I will not leave a secure computer application unattended while signed on.
9. I will comply with all policies and procedures and other rules of Sands Point Physical Therapy relating to confidentiality of information and sign-on codes.
10. I understand that my use of the system will be periodically monitored to ensure compliance with this agreement.
11. I agree not to sue the information in any way detriment to the organization and will keep all such information confidential.
12. I will not disclose protected health information or other information that is considered proprietary, sensitive or confidential unless there is a need to know basis.
13. I will limit distribution of confidential information to only parties with a legitimate need in performance of the organizations mission
14. I agree that disclosure of confidential information is prohibited indefinitely, even after termination of employment or business relationship, unless specifically waived in writing by the authorized party
15. This agreement shall survive the termination expiration or cancellation of this agreement

I further understand that if I violate any of the above terms, I may be subject to disciplinary action, including discharge. Loss of privilege, termination of contract, legal action for monetary damages or injunction or both or any other remedy available to Sands Point Physical Therapy.

Employee Name_____ Date _____

Employee Signature:_____

SS #_____

HIPAA Privacy Policies and Laws

The U.S. Department of Health and Human Services (“HHS”) issued the Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”).[1] The Privacy Rule standards address the use and disclosure of individuals’ health information—called “protected health information” by organizations subject to the Privacy Rule — called “covered entities,” as well as standards for individuals' privacy rights to understand and control how their health information is used.

A major goal of the Privacy Rule is to assure that individuals’ health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well-being.

What Information is Protected

Protected Health Information. The Privacy Rule protects all *"individually identifiable health information"* held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information (PHI)."[12]

“Individually identifiable health information” is information, including demographic data, that relates to:

the individual’s past, present or future physical or mental health or condition,

the provision of health care to the individual, or

the past, present, or future payment for the provision of health care to the individual,

and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.[13] Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

Summary of the HIPAA Privacy Rule

This is a summary of key elements of the Privacy Rule including who is covered, what information is protected, and how protected health information can be used and disclosed. Because it is an overview of the Privacy Rule, it does not address every detail of each provision.

Introduction

The *Standards for Privacy of Individually Identifiable Health Information* (“Privacy Rule”) establishes, for the first time, a set of national standards for the protection of certain health information. The U.S. Department of Health and Human Services (“HHS”) issued the Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”).[1] The Privacy Rule standards address the use and disclosure of individuals’ health information—called “protected health information” by organizations subject to the Privacy Rule — called “covered entities,” as well as standards for individuals' privacy rights to understand and control how their health information is used. Within HHS, the Office for Civil Rights (“OCR”) has responsibility for implementing and enforcing the Privacy Rule with respect to voluntary compliance activities and civil money penalties.

A major goal of the Privacy Rule is to assure that individuals’ health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well-being. The Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing. Given that the health care marketplace is diverse, the Rule is designed to be flexible and comprehensive to cover the variety of uses and disclosures that need to be addressed.

This is a summary of key elements of the Privacy Rule and not a complete or comprehensive guide to compliance. Entities regulated by the Rule are obligated to comply with all its applicable requirements and should not rely on this summary as a

source of legal information or advice. To make it easier for entities to review the complete requirements of the Rule, provisions of the Rule referenced in this summary are cited in the end notes. Visit our Privacy Rule section to view the entire Rule, and for other additional helpful information about how the Rule applies. In the event of a conflict between this summary and the Rule, the Rule governs.

Statutory and Regulatory Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, was enacted on August 21, 1996. Sections 261 through 264 of HIPAA require the Secretary of HHS to publicize standards for the electronic exchange, privacy and security of health information. Collectively these are known as the *Administrative Simplification* provisions.

HIPAA required the Secretary to issue privacy regulations governing individually identifiable health information, if Congress did not enact privacy legislation within three years of the passage of HIPAA. Because Congress did not enact privacy legislation, HHS developed a proposed rule and released it for public comment on November 3, 1999. The Department received over 52,000 public comments. The final regulation, the Privacy Rule, was published December 28, 2000.[2]

In March 2002, the Department proposed and released for public comment modifications to the Privacy Rule. The Department received over 11,000 comments. The final modifications were published in final form on August 14, 2002.[3] A text combining the final regulation and the modifications can be found at 45 CFR Part 160 and Part 164, Subparts A and E.

Who is Covered by the Privacy Rule

Health Care Providers. Every health care provider, regardless of size, who electronically transmits health information in connection with certain transactions, is a covered entity. These transactions include claims, benefit eligibility inquiries, referral authorization requests, or other transactions for which HHS has established standards under the HIPAA Transactions Rule.[6] Using electronic technology, such as email, does not mean a health care provider is a covered entity; the transmission must be in connection with a standard transaction. The Privacy Rule covers a health care provider whether it electronically transmits these transactions directly or uses a billing service or other third party to do so on its behalf. Health care providers include all “providers of services” (e.g., institutional providers such as hospitals) and “providers of medical or health services” (e.g., non-institutional providers such as physicians, dentists and other practitioners) as defined by Medicare, and any other person or organization that furnishes, bills, or is paid for health care.

What Information is Protected

Protected Health Information. The Privacy Rule protects all *"individually identifiable health information"* held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information (PHI)."[12]

“Individually identifiable health information” is information, including demographic data, that relates to:

the individual’s past, present or future physical or mental health or condition,

the provision of health care to the individual, or

the past, present, or future payment for the provision of health care to the individual,

and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.[13] Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g.

De-Identified Health Information. There are no restrictions on the use or disclosure of de-identified health information.[14] De-identified health information neither identifies nor provides a reasonable basis to identify an individual. There are two ways to de-identify information; either: (1) a formal determination by a qualified statistician; or (2) the removal of specified identifiers

of the individual and of the individual's relatives, household members, and employers is required, and is adequate only if the covered entity has no actual knowledge that the remaining information could be used to identify the individual.[15]

General Principle for Uses and Disclosures

Basic Principle. A major purpose of the Privacy Rule is to define and limit the circumstances in which an individual's protected heath information may be used or disclosed by covered entities. A covered entity may not use or disclose protected health information, except either: (1) as the Privacy Rule permits or requires; or (2) as the individual who is the subject of the information (or the individual's personal representative) authorizes in writing.[16]

Required Disclosures. A covered entity must disclose protected health information in only two situations: (a) to individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their protected health information; and (b) to HHS when it is undertaking a compliance investigation or review or enforcement action.[17] See additional guidance on Government Access.

Permitted Uses and Disclosures

Permitted Uses and Disclosures. A covered entity is permitted, but not required, to use and disclose protected health information, without an individual's authorization, for the following purposes or situations: (1) To the Individual (unless required for access or accounting of disclosures); (2) Treatment, Payment, and Health Care Operations; (3) Opportunity to Agree or Object; (4) Incident to an otherwise permitted use and disclosure; (5) Public Interest and Benefit Activities; and (6) Limited Data Set for the purposes of research, public health or health care operations.[18] Covered entities may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make.

(1) To the Individual. A covered entity may disclose protected health information to the individual who is the subject of the information.

(2) Treatment, Payment, Health Care Operations. A covered entity may use and disclose protected health information for its own treatment, payment, and health care operations activities.[19] A covered entity also may disclose protected health information for the treatment activities of any health care provider, the payment activities of another covered entity and of any health care provider, or the health care operations of another covered entity involving either quality or competency assurance activities or fraud and abuse detection and compliance activities, if both covered entities have or had a relationship with the individual and the protected health information pertains to the relationship. See additional guidance on Treatment, Payment, & Health Care Operations.

Treatment is the provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultation between providers regarding a patient and referral of a patient by one provider to another.[20]

Payment encompasses activities of a health plan to obtain premiums, determine or fulfill responsibilities for coverage and provision of benefits, and furnish or obtain reimbursement for health care delivered to an individual[21] and activities of a health care provider to obtain payment or be reimbursed for the provision of health care to an individual.

Health care operations are any of the following activities: (a) quality assessment and improvement activities, including case management and care coordination; (b) competency assurance activities, including provider or health plan performance evaluation, credentialing, and accreditation; (c) conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs; (d) specified insurance functions, such as underwriting, risk rating, and reinsuring risk; (e) business planning, development, management, and administration; and (f) business management and general administrative activities of the entity, including but not limited to: de-identifying protected health information, creating a limited data set, and certain fundraising for the benefit of the covered entity.[22]

Authorized Uses and Disclosures

Marketing. Marketing is any communication about a product or service that encourages recipients to purchase or use the product or service.[49] The Privacy Rule carves out the following health-related activities from this definition of marketing:

Communications to describe health-related products or services, or payment for them, provided by or included in a benefit plan of the covered entity making the communication;

Communications about participating providers in a provider or health plan network, replacement of or enhancements to a health plan, and health-related products or services available only to a health plan's enrollees that add value to, but are not part of, the benefits plan;

Communications for treatment of the individual; and

Communications for case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or care settings to the individual.

Marketing also is an arrangement between a covered entity and any other entity whereby the covered entity discloses protected health information, in exchange for direct or indirect remuneration, for the other entity to communicate about its own products or services encouraging the use or purchase of those products or services. A covered entity must obtain an authorization to use or disclose protected health information for marketing, except for face-to-face marketing communications between a covered entity and an individual, and for a covered entity's provision of promotional gifts of nominal value. No authorization is needed, however, to make a communication that falls within one of the exceptions to the marketing definition. An authorization for marketing that involves the covered entity's receipt of direct or indirect remuneration from a third party must reveal that fact. See additional guidance on Marketing.

Notice and Other Individual Rights

Privacy Practices Notice. Each covered entity, with certain exceptions, must provide a notice of its privacy practices.[51] The Privacy Rule requires that the notice contain certain elements. The notice must describe the ways in which the covered entity may use and disclose protected health information. The notice must state the covered entity's duties to protect privacy, provide a notice of privacy practices, and abide by the terms of the current notice. The notice must describe individuals' rights, including the right to complain to HHS and to the covered entity if they believe their privacy rights have been violated. The notice must include a point of contact for further information and for making complaints to the covered entity. Covered entities must act in accordance with their notices. The Rule also contains specific distribution requirements for direct treatment providers, all other health care providers, and health plans. See additional guidance on Notice.

Notice Distribution. A covered health care provider with a *direct treatment* relationship with individuals must have delivered a privacy practices notice to patients starting April 14, 2003 as follows:

- Not later than the first service encounter by personal delivery (for patient visits), by automatic and contemporaneous electronic response (for electronic service delivery), and by prompt mailing (for telephonic service delivery);
- By posting the notice at each service delivery site in a clear and prominent place where people seeking service may reasonably be expected to be able to read the notice; and
- In emergency treatment situations, the provider must furnish its notice as soon as practicable after the emergency abates.

Administrative Requirements

HHS recognizes that covered entities range from the smallest provider to the largest, multi-state health plan. Therefore, the flexibility and scalability of the Rule are intended to allow covered entities to analyze their own needs and implement solutions appropriate for their own environment. What is appropriate for a particular covered entity will depend on the nature of the covered entity's business, as well as the covered entity's size and resources.

Privacy Policies and Procedures. A covered entity must develop and implement written privacy policies and procedures that are consistent with the Privacy Rule.[64]

Privacy Personnel. A covered entity must designate a privacy official responsible for developing and implementing its privacy policies and procedures, and a contact person or contact office responsible for receiving complaints and providing individuals with information on the covered entity's privacy practices.[65]

Workforce Training and Management. Workforce members include employees, volunteers, trainees, and may also include other persons whose conduct is under the direct control of the entity (whether or not they are paid by the entity).[66] A covered entity must train all workforce members on its privacy policies and procedures, as necessary and appropriate for them to carry out their functions.[67] A covered entity must have and apply appropriate sanctions against workforce members who violate its privacy policies and procedures or the Privacy Rule.[68]

Enforcement and Penalties for Noncompliance

Compliance. The Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) establishes a set of national standards for the use and disclosure of an individual's health information – called protected health information – by covered entities, as well as standards for providing individuals with privacy rights to understand and control how their health information is used. The Department of Health and Human Services, Office for Civil Rights (OCR) is responsible for administering and enforcing these standards and may conduct complaint investigations and compliance reviews.

Consistent with the principles for achieving compliance provided in the Privacy Rule, OCR will seek the cooperation of covered entities and may provide technical assistance to help them comply voluntarily with the Privacy Rule. Covered entities that fail to comply voluntarily with the standards may be subject to civil money penalties. In addition, certain violations of the Privacy Rule may be subject to criminal prosecution. These penalty provisions are explained below.

Civil Money Penalties. OCR may impose a penalty on a covered entity for a failure to comply with a requirement of the Privacy Rule. Penalties will vary significantly depending on factors such as the date of the violation, whether the covered entity knew or should have known of the failure to comply, or whether the covered entity's failure to comply was due to willful neglect. Penalties may not exceed a calendar year cap for multiple violations of the same requirement.

	For violations occurring prior to 2/18/2009	**For violations occurring on or after 2/18/2009**
Penalty Amount	Up to $100 per violation	$100 to $50,000 or more per violation
Calendar Year Cap	$25,000	$1,500,000

A penalty will not be imposed for violations in certain circumstances, such as if:

the failure to comply was not due to willful neglect, and was corrected during a 30-day period after the entity knew or should have known the failure to comply had occurred (unless the period is extended at the discretion of OCR); or

the Department of Justice has imposed a criminal penalty for the failure to comply (see below).

In addition, OCR may choose to reduce a penalty if the failure to comply was due to reasonable cause and the penalty would be excessive given the nature and extent of the noncompliance.

Before OCR imposes a penalty, it will notify the covered entity and provide the covered entity with an opportunity to provide written evidence of those circumstances that would reduce or bar a penalty. This evidence must be submitted to OCR within 30 days of receipt of the notice. In addition, if OCR states that it intends to impose a penalty, a covered entity has the right to request an administrative hearing to appeal the proposed penalty.

Criminal Penalties. A person who knowingly obtains or discloses individually identifiable health information in violation of the Privacy Rule may face a criminal penalty of up to $50,000 and up to one-year imprisonment. The criminal penalties increase to $100,000 and up to five years imprisonment if the wrongful conduct involves false pretenses, and to $250,000 and up to 10 years imprisonment if the wrongful conduct involves the intent to sell, transfer, or use identifiable health

information for commercial advantage, personal gain or malicious harm. The Department of Justice is responsible for criminal prosecutions under the Privacy rules

I, _____, have read the HIPPA Privacy rules and privacy practices in effect at Sands Point Physical Therapy.

I understand that I am responsible for ensuring the security, integrity and confidentiality of patient health information created, obtained and /or maintained by Sands Point physical Therapy.

I have reviewed, understand and agree to abide by the following policies:

1. General Privacy
2. Patient Privacy Rights
3. Uses and Disclosures of Protected health Information
4. Minimum Necessary information
5. Administrative, Technical and Physical Safeguards
6. Uses and Disclosures for Research Purposed & Waivers
7. De-identification of Identifiable Patient information and use of Limited Data Sets
8. Business Associate Relationships
9. Enforcement, Sanctions and Penalties for Violations of Individual Privacy

- **I understand that non-compliance will be cause for disciplinary action up to and including termination form Sands Point Physical Therapy and possible legal actions for violations of applicable regulations and laws.**

I agree to promptly report all violation or suspected violations of any of the above policies to Sands Point Physical Therapy's Privacy Officer through the designated reported channels.

Employee Name:_____

Employee Signature:_____

Date:_____