results
PHYSIOTHERAPY

HIPAA
The Health Insurance Portability and Accountability Act of 1996

Results Physiotherapy's policy regarding privacy and security of protected health information (PHI) is a reflection of our commitment to protecting the confidentiality of patients' medical records, patient accounts, clinical information from management information systems, confidential conversations and any other sensitive material.

While a commitment of privacy and security of PHI is an expectation, there remains a possibility that an inappropriate or unintended disclosure of PHI may result in a privacy breach. This training will help you determine the procedure to mitigate all breaches, both willful violations and unintended actions, consistent with guidance described by the HIPAA and HITECH rules.

results PHYSIOTHERAPY

What is HIPAA?

HIPAA is The Health Insurance Portability and Accountability Act of 1996

What is the primary purpose of the HIPAA privacy rule?

The rule protects from unauthorized disclosure of any personally-identifiable health information (protected health information or PHI) that pertains to a patients health.

What is a covered entity?

Covered entities under the HIPAA Privacy Rule must comply with the Rule's requirements for safeguarding the privacy of protected health information.

There are three specific groups that refers to covered entity

Healthcare Providers

Health Plans

Healthcare Clearinghouses

Business Associates and Business Associate Subcontractors

A “business associate” is a person or entity, other than a member of the workforce of a covered entity, that delegates functions, actions and services to subcontractors and individuals and entities outside of the business associate’s workforce.
HIPAA requires agreements between business associates and their subcontractors providing that the subcontractor is subject to the same HIPAA requirements concerning access to and use of protected information as the business associate.
Subcontractors are contractually obligated to comply with HIPAA requirements but they are not directly subject to HIPAA.

What is Protected Health Information (PHI) and (ePHI) under HIPAA?

Under the HIPAA Privacy Rule protected health information (PHI) refers to individually identifiable health information. Individually identical health information is that which can be linked to a particular person.
Common identifiers of health information include

- Full Names; in combination with
- Social security numbers
- Addresses
- Dates of birth

HIPAA Privacy

A covered entity may use or disclose an individual's PHI only under these conditions:

- To communicate directly with the individual about their PHI
- With the individual's written authorization or other legal agreement
- Without the individual's authorization for treatment, payment and operations.
- If allowed by state law, medical information may be disclosed to a child's parent or guardian.
- When using or disclosing PHI or when requesting PHI from another covered entity or business associate, you must make reasonable efforts to limit use or disclosure as much as possible.

results PHYSIOTHERAPY

Reasonable Safeguards to Protect PHI

- Be cognizent of your surrounding when discussing individuals PHI
- Do not use names of individuals whose PHI is being discussed
- Keep PHI secure at workstations and public spaces
- Lock computers with password protection when not in use

results PHYSIOTHERAPY

Notice of Privacy Practices

Covered entities must provide individuals with notice that tells them how their health information can be used and how they can exercise their privacy rights. Notices must be given to patients at their first visit

Using PHI for Marketing Purposes

Results Physiotherapy cannot disclose individuals PHI for marketing purposes unless the individual has given written consent

The only exceptions are

- Treatment of the individual (referrals)
- Case management or care coordination for the individual, or to direct or recommend alternative treatments, health care providers or settings of care to the individual

results PHYSIOTHERAPY

HIPAA Security Rule

What is the HIPAA Security Rule?

- Requires the safeguards, both physical and electronic, to ensure the secure passage, maintenance and reception of protected health information (PHI).

The primary goals of the HIPAA Security rule

- Maintenance of the privacy and availability of ePHI created, received, transmitted and maintained
- Protection of the ePHI from anticipated hazards and risks that may compromise it's security and integrity
- Ensure that protection ePHI from wrongful disclosure or use as specified under the Privacy Rule

Administrative Safeguards

Administrative safeguards are “administrative actions” and policies and procedures to manage the selection, development, implementation and maintenance of security measures to protect ePHI and to manage the conduct of the covered entity’s workforce in relation to the protection of that information.

Ways that Results Physiotherapy ensures administrative safeguards

- Privacy Officer
- Contingency Plan
- BA contracts in place
- Termination procedures

Definition of Breach

A **“breach”** is an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual. There are three exceptions to the definition of “breach.”

- Unintentional acquisition, access, or use of protected health information by a workforce member acting under the authority of a covered entity or business associate.
- Inadvertent disclosure of protected health information from a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate or
- If the covered entity or business associate has a good faith belief that the unauthorized Individual, to whom the impermissible disclosure was made, would not have been able to retain the information.

results PHYSIOTHERAPY

Required Reporting Responsibilities

Anyone who is aware of or suspects a violation of privacy/security policy or a breach of patient information is required to report it immediately to The Privacy Officer.
Once the initial report is made, others should be informed including: Immediate Supervisor and Manager of the department

Reporting a violation or breach in bad faith or for malicious reasons may be interpreted as a misuse of the reporting notification and may result in disciplinary action.

Investigations of Reported Breaches

All reported violations will be assessed by the Privacy Officer.

When applicable, the Privacy Officer will take necessary steps in the event that any confidential or restricted data is compromised.
If the PHI in question is not indecipherable, unreadable or unusable and falls into unauthorized hands, Results Physiotherapy will determine through a risk assessment whether the disclosure caused a significant risk of financial, reputational or other harm to the individual.

Outcomes of the harm threshold risk analysis are documented and acted upon accordingly, as outline in the Breach protocol.
Information pertaining to investigations of breaches will only be shared with those who need to know. The investigator(s) will conduct the necessary and appropriate investigation commensurate with the level of breach and the specific facts. The investigation may include, but is not limited to, interviewing the individuals involved, interviewing other individuals, obtaining specific facts surrounding the violation/breach and reviewing pertinent documentation.

Disciplinary Sanctions and Appeals

If the individual responsible for the violation/breach is a Business Associate, Results Physiotherapy will take reasonable corrective steps to implement sanctions. While Results Physiotherapy is not required to monitor the activity of our Business Associates, we will address problems as they rise and request that our Business Associates remedy their behavior. Results Physiotherapy reserves the right to termination contracts if it becomes clear that the business partner cannot be relied upon to maintain the privacy/security of information we provide to them.

results PHYSIOTHERAPY

Documentation and Tracking of Breaches

All information documenting the process required under HIPAA Privacy and Security and HITECH law regarding the violation or breach will be retained for a period of six (6) years by the Privacy Officer.

Violations that meet the definition of breach under the HITECH Act are reported as required to the Department of Health and Human Services office of Civil Rights.

Questions?

If you have questions regarding privacy and security, please contact Human Resources at hr@resultsphysiotherapy.com