Morgan Support Services

HIPAA Information

What is HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA,) a federal law passed in 1996 that affects health care and insurance industries. Morgan Support Services falls under the "health care" designation. You probably have signed HIPAA forms at your doctor's office because your medical information is protected by HIPAA as well.

HIPAA has several elements, including privacy, security, and electronic claims processing.

- The Privacy Rule requires us to protect the privacy and confidentiality of protected health information (PHI) and requires us to implement security safeguards to protect PHI in all forms
- The Security Rule requires us to protect the confidentiality, integrity, and availability of electronic PHI and outlines administrative, physical, and technical safeguards to protect PHI stored or processed electronically.

What is the Identity Theft Protection Act?

The Identity Theft Protection Act (ITPA) is a North Carolina law that imposes certain obligations on NC state agencies and NC businesses concerning the collection, use, and dissemination of social security numbers and other personal identifying information (PII.)

- It requires the protection of personal information or identifiers from inappropriate disclosures for both patients and and employees.
- It requires a business to to notify individuals when it becomes aware that certain information has been inappropriately disclosed.

What is the difference between PHI, PII, Confidential, and Internal Information?

- Protected Health Information (PHI) is any health information that can be used to identify a person and which relates to the person, services the person receives, or payments for those services. Examples of PHI include demographic, medical, financial, and personal identification information.
- Personal Identifying Information (PII) as defined in the Identity Theft Protection Act includes such things as social security numbers, driver's license numbers, checking or savings account numbers, credit or debit card numbers, biometric data, fingerprints, and passwords.
- Confidential Information is very important and highly sensitive material that is not classified as PHI. This information is of a private or otherwise sensitive nature and must be restricted to those with a legitimate business needs for access. Examples of Confidential Information may include personnel information, key financial information, proprietary information of commercial research sponsors, system access passwords, and information file encryption keys.
- Internal Information is information that is intended for unrestricted use within a business, and in some cases within affiliated organizations and business partners. This is information that can be shared throughout the business without advanced approval from the information owner. One example of Internal Information is a personnel directory.

What type of Privacy/Security Training must I complete and how often?
New employees, volunteers, contractors, and interns at Morgan Support Services must receive training in confidentiality and sign a confidentiality agreement prior to being allowed access to confidential information. The training and confidentiality agreement must be repeated at least annually.

What PHI may I access and/or disclose?
ith some exceptions, you may use or share PHI as is required by your job description. Only the limited amount of PHI necessary should be used. For example, there is no need to include social security numbers on any of the paperwork that we produce; therefore that is not information for which you are likely to ever have need of access. Accessing information outside of your job responsibilities is considered a violation of the agency's Privacy and Information Security policies.

- May I access my own records? You are able to access your records such as are made available through your Paychex Flex account. The Personnel Director may assist you in accessing any other records.
- May I access a family member's records? You may not access any information outside of your job responsibilities. You must have written authorization to access a family member's records. Although that scenario is unlikely to arise through your work at Morgan Support Services, you may encounter the need to know this information in your personal life if you are assisting a family member with his/her medical care.

What is an incidental disclosure?
An incidental use or disclosure is a secondary use or exposure that cannot reasonably be prevented, is limited in nature, and that occurs as a result of another use or disclosure that is permitted by the HIPAA Privacy Rule. The HIPAA Privacy Rules permits certain incidental uses and disclosures that occur as a by-product of another person's permissible or required use or disclosure, so long as reasonable safeguards are applied and the maximum necessary standards are implemented with respect to primary use or disclosure. An example might be if, during his/her team meeting, a person we support mentions the name of a peer from the day support program.

Maintaining Confidentiality
Morgan Support Services has policies in place that dictate what information may be shared by whom, with whom, in what manner, and under what situations. So long as you follow agency policies and ask questions if you are in doubt about how the policies apply to you, you should be in compliance with all relevant HIPAA requirements. Policies address conversations you may have with others inside and outside of the facility, things you write down, paper and electronic documents and files, and social media.

People who receive services through Morgan Support Services and/or their guardians are provided with information regarding how our agency protects confidential information.

Morgan Support Services

HIPAA Information

Electronic Records

If you, through the course of your regular or otherwise assigned job duties, are given the responsibility for creating, saving, storing, and/or accessing electronic documents regarding the people we support or our employees, you will be given specific instructions regarding the policies and procedures that Morgan Support Services has implemented for ensuring the privacy, integrity, and accessibility of those electronic documents. Whenever you use any electronic system, such as MSS' Electronically Generated Goalsheets (EGGs) you must follow all policies and procedures to ensure that you are in compliance with HIPAA regulations.

You must ensure that

- you create strong passwords to protect information you are responsible for storing.
- you share those passwords with the Executive Director.
- you keep those passwords secret from all others.
- you follow the regulations set forth by the IT Contractor regarding use of laptops and remote access to the agency's server.
- unless otherwise instructed, you keep all electronic equipment that includes confidential information stays in secured locations within the facility at all time.
- report any possible breach of confidentiality to the Executive Director or Quality Enhancement Director as soon as you are aware of it.

For EGGs and other DocuSign documents, you must be sure that you are the only person who has access to the password for the email account that you use. If you prefer, MSS will set you up with a work-only email to use for these activities.

The IT Contractor is responsible for the disposal of any equipment or devices which may hold confidential information when the equipment or devices are no longer in use. You are responsible to turn all such equipment and devices over to the Executive Director when you are no longer using them.

As long as you follow the policies and procedures you are given regarding the creation and storage of, and access to, electronic records, and ask questions if you are not clear about how the policies and procedures apply to you, you should be in compliance with maintaining the confidentiality of those records.

Your Responsibilities

- Take Morgan Support Services' policies and procedures regarding confidentiality and privacy seriously.
- You are responsible for maintaining the confidentiality of all information to which you are exposed through your employment with Morgan Support Services.
- You are responsible for asking questions when you don't understand the policies or procedures, or when you are unsure as to how they apply to you.

You are responsible to report any possible breaches of confidentiality immediately to the Executive Director or the Quality Enhancement Director. You will be held responsible for not reporting potential breaches of confidentiality even if those breaches are not a result of anything you did or did not do if it is discovered that you were aware of the potential.

The people we support deserve the same respect that you do when you visit a doctor. Think about how you would feel if you found out your doctor was discussing your medical files at home or in public in such a way that others knew your personal medical information. Protect the privacy of the people we support the way you expect others to protect your privacy.