HEALTH FORCE LLC

HIPAA PRIVACY COMPLIANCE POLICY

Overview: Privacy compliance involves fulfilling the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), its subsequent amendments, and any related legislation such as the Health Information Technology for Economic and Clinical Health (HITECH) Act. These laws require that Health Force employ technical, physical, and administrative safeguards to protect an individual's protected health information (PHI) and that should a breach occur there is a sufficient notification procedure.

Protected Information: PHI includes any information that we create, maintain, or receive that contains data elements or a combination of data elements that could identify a person or provides a reasonable basis to believe someone could be identified (known as identifiers), contains health-related information, and is maintained or transmitted in any form (*i.e.*, electronic, written, or oral).

For example, individually identifiable information (*i.e.*, personal information) typically includes: name, SSN, biometric records, date of birth, driver's license, email address. Whereas, health information typically includes diagnosis, procedure code, treating physician, prescribed medications, or dates of service. Accordingly, PHI would generally be considered to be some combination of both personal information and health information. To the extent such information is accessible to Health Force, we also protect a client's financial information, which typically includes credit card numbers, bank account numbers, credit score, or even payment history.

Purpose and Applicability: This policy is applicable to all Health Force employees and contracts. It details the requirements of federal laws regulating privacy and certain information and how that information can be disclosed, safeguards to protect against inadvertent disclosure, and procedures to address disclosure.

This policy does not apply to certain Health Force actions or activities that does not require authorized disclosure. These activities include:

- Use of PI, PHI, and PFI for the proper management and administration of Health Force business operations
- Use of PI, PHI, and PFI for data aggregation and analysis purposes relating to Health Force business operations
- Use of PI, PHI and PFI to report violations to the appropriate Federal and State authorities consistent with HIPAA requirements

Authentication: Health Force requires authentication prior to disclosure of any protected health information. Authentication is a two-step process validating both identity and authority. Both are required elements of the authentication process. We must verify the identity of the individual for whom information is being requested. We must also verify the authority of any person to have access to protected health information.

For example, when we ask for full name, date of birth, zip code we are validating that the caller knows the identity of the member whose PHI is being requested.

Minimum Necessary: After a caller is authenticated, information should still be released on a minimum necessary basis. Minimum necessary is defined as the limited use and disclosure of protected information to the least amount required to accomplish the intended purpose of the use, disclosure or request. This includes uses and disclosures by business associates from another covered entity.

Safeguards: Regardless of where you work, telework, home office, or at Health Force's office, you are required to follow the below Health Force safeguards:

- Do not leave personal health information openly displayed on your work surface when you are away from your work space during the day.
- Always make sure your computer is password protected and be sure to lock your computer screen when you are away from your work area.
- Clean your work space of all personal health information at the end of the day.
- Secure all personal health information in a locked container, desk, file cabinet, or storage unit at the end of the day.
- Properly dispose of PHI by deleting or shredding any information that is no longer necessary for your specific job function, provided such information does not need to be retained for record retention purposes.
- Do not place discarded personal health information into a trash receptacle.
- Do not allow anyone else to access your laptop before you have properly secured any client's PHI.
- Passwords are to be kept confidential at all times.
- Laptops are to be secured in a locked area when not being used.
- Do not use a speaker phone when discussing personal and health information.
- Avoid discussion of confidential information in public areas, including elevators, break rooms, and waiting rooms.
- Do not check laptop as baggage when traveling.
- Never use a third-party location, such as Staples, Kinko's, or Office Max to print confidential information.
- If sending a fax, always use a cover page with the minimum necessary amount of information.
- Do not leave a laptop or paper documents in a vehicle overnight, including in a trunk.
- Please review and adhere to Health Force's Computer, E-mail, and Internet Access Policy as it relates to PHI.

Breach Disclosure: HIPAA requires Health Force to document all instances of privacy concerns and violations. A privacy incident occurs when an individual's protected information is used or disclosed inappropriately or without his/her permission. In accordance with HIPAA, it is the Compliance Department's responsibility to investigate and determine if the incident is classified as a breach and to take appropriate action as required.

Causes of a privacy incident may vary and could be the result of:

- A system error
- A clerical error
- Malicious intent by an individual

The following are examples of privacy incidents that should be reported to the Compliance Department.

- Medical release forms or medical records were sent to wrong individual
- Faxes containing PHI were sent to the wrong individual, client, vendor, or provider

.

Reporting a Privacy Incident

- When: All privacy incidents must be promptly reported.
- How/What: Notify the Compliance Department via email (corporatecompliance@healthforceus.com) or phone (1.877.244.9151 ext. 720) and be sure to be as detailed as possible and may arrangements to securely provide the Compliance Department with all necessary documentation.
- Why: Reporting of a privacy incident is required by federal and state privacy regulations, and it is the right thing to do.

Individual Privacy Rights

- Right to access, inspect, and copy PHI maintained by a business associate of a covered entity.
- Right to obtain an accounting of disclosures of his/her PHI
- Right to request a restriction on the use of his/her PHI
- Right to remove a previous restriction of PHI
- Right to request an amendment of his/her PHI
- Right to request alternative communication methods of his/her PHI
- Right to file a complaint about any violation of his/her privacy

Privacy Complaints: If you receive a request or notice that a client wants to file a privacy complaint or wished to invoke one of his/her individual privacy rights, please inform the individual that a member of the Compliance Department will follow up with them directly. Please also provide the following information to the complainant as well

1.877.244.9151 ext. 720

corporatecompliance@healthforceus.com

or send a written complaint to

Health Force, LLC
1335 Elm Abode Terrace
Columbia, SC 29210

Disciplinary Action: Employees who violate or fail to comply with these policies and procedures will be subject to disciplinary action, up to and including termination of employment and may be subject to civil and criminal penalties.

No Retaliation for Reporting: Health Force will not intimidate, threaten, coerce, discriminate against, or take other retaliatory actions against individuals exercising their individual rights, or anyone submitting a privacy complaint, or participating in any investigation or review.