Executive Offices
8465 Merchants Way.
Suite 206
Jacksonville, FL 32222

Laboratory
1122 Cambridge Square.
Suite E
Alpharetta, GA 30009

Privacy Policies

JANAUARY 2022

SECURITY OF INFORMATION SENT BY FAX

PURPOSE:

Confidential health information that is sent by fax must be afforded the same level of information security as any other form of individually identifiable health information.

POLICY:

It is the policy of HeliosDX to take reasonable precautions to protect the confidentiality and security of confidential health information sent by fax.

PROCEDURE:

The ability to fax confidential information helps in the timely discharge of the essential business functions of HeliosDX. HeliosDX's fax software solution is for the sole use of HeliosDX personnel for the purposes of conducting Agency business. Personal use of the fax machines is normally prohibited with the exception of limited personal use (the sending of a single fax) to deal with a personal emergency with the prior authorization of the Director of Administrative Services.

All faxes sent in the course of Agency business must have a cover sheet that identifies the names and fax numbers of both sender and intended recipient. In addition, the cover sheet should include the following disclaimer:

"This fax is confidential and intended solely for the use of the individual or entity to which it is addressed. If you have received this fax in error, please notify the sender immediately. Please note that any views or opinions presented in this fax are solely those of the author and do not necessarily represent those of HeliosDX."

Before sending a fax, employees must call the intended recipient of the fax to ensure that the recipient is available to receive the fax, verify that the correct fax number has been identified, and that the receiving fax machine is in a secure location. For especially sensitive information, confirmation of safe receipt of the fax should also be sought.

CONFIDENTIALITY OF PATIENT FILES

Written records and other information/ files about patients will not be released outside of HeliosDX, without written permission of the patient and his/her parent or legal guardian, except to funding agencies, insurance agencies, or in response to a subpoena, court order or governmental agency request. Confidential information about a patient will not be provided over the telephone or in person without the patient's or legal guardian's consent, unless HeliosDX is legally required to disclose such information. Only those employees at HeliosDX with a legitimate business need to know will have access to the patient's written records and other confidential information and files.

PURPOSE:

To protect the privacy of confidential patient information by HeliosDX and to encourage patients to accept services and build a relationship of trust based upon the assurance of confidentiality.

PROCEDURE:

- All records shall be kept secure, with access limited to staff with a legitimate business need.
- Only staff participating in the development, provision, or supervision of the patient's treatment will have access to the records. However, appropriate clerical and administrative staff will be allowed access, but will be bound by the same requirements for confidentiality.
- Information contained in the written files will be released to another agency only with the written consent of the patient, and of the parent or legal guardian.
- All subpoenas or court orders must be brought to the attention of the Director of Administrative Services. The Director of Administrative Services will consult with HeliosDX's legal counsel for an appropriate response.

NON-DISCLOSURE/CONFIDENTIALITY OF BUSINESS INFORMATION

The protection of confidential and proprietary business information and trade secrets (that does not fall within the protection of HIPAA as discussed in this Handbook) is vital to the interests and the success of HeliosDX. Employees who improperly use or disclose trade secrets or confidential and proprietary business information will be subject to discipline, up to and including termination of employment.

Confidential and proprietary information and trade secrets, includes, but is not limited to operational, marketing, business plans, strategies and projections, analyses, studies, programs and program development, financial statements and information, economic data or information, billing, records and data, accounting, budgets, expenses, vendor/supplier contracts, computer programs, internal security codes and passwords, patient lists, training information, , information protected by copyright and any other information belonging to RPG that is marked as "Confidential" or "Proprietary," or that otherwise could reasonably be considered confidential or proprietary to HeliosDX or a trade secret.

SEARCH WARRANTS

PURPOSE:

To define how HeliosDX will respond to search warrants that allow law enforcement officers the ability to search a specific area and/or seize property as outlined in the search warrant.

POLICY:

HeliosDX is subject to federal, state, and local regulatory agencies, government agencies, and law enforcement personnel. If a staff member is presented with a written court order from a law enforcement officer requesting to search any area within HeliosDX, the company's owners, Director of Administrative Services, and Director of Clinical Services must be notified immediately.

PROCEDURE:

- If a representative from either entity presents HeliosDX with a search warrant, the owners, Director of Administrative Services, and Director of Clinical Services must be notified immediately.
- Law enforcement officers should be informed that the appropriate persons have been contacted and asked to wait until the owner (s), Director of Administrative Services, and/or Director of Clinical Services arrives.
- If the officers cannot wait, present members of the management team must comply with the search warrant.

HIPAA:
Individual Responsibility for the Protection of Patient Privacy and for the Security and Integrity of Protected Health Information

PURPOSE:

To establish the requirements for each employee to protect patients' privacy rights and safeguard their individually identifiable health information as required by the Health Insurance Portability and Accountability Act (HIPAA), Standards for Privacy and Security of Individually Identifiable Health Information, 45 CFR Parts 160 and 164 and all other applicable Federal regulations and interpretive guidelines.

POLICY:

Each employee of HeliosDX has a responsibility to patients and HeliosDX to uphold patients' privacy rights, and maintain the security and integrity of their protected health information. Patient's personal health information will be treated as confidential, and held, used and disclosed only within applicable regulations. All employees will collect, use, disclose, maintain and store patients' protected health information in an honest, ethical, secure, and confidential manner as required by law.

PROCEDURE:

All Agency employees will uphold and safeguard the rights of patients to the privacy of their personal health information by ensuring that individually identifiable information is used and disclosed only under the following conditions:

- Staff will take all reasonable precautions as required by law to safeguard the confidentiality of patients' protected health information.
- Use and disclosure is permitted without specific authorization when required for treatment, payment, and healthcare operations on the terms set out in HeliosDX's current Notice of Privacy Practices.
- Disclosure to any person or entity for other purposes may be made on written authorization of the patient or, if appropriate, his/her parent or legal guardian. Authorization must be obtained, which must be completed in its entirety.
- Use and disclosure of health information for other purposes without authorization may be made only when required by law and under conditions set out in the current Notice of Privacy Practices and Disclosure of Health Information Without Authorization;

All Agency employees will comply with all applicable policies and procedures implemented to ensure the security and integrity of patients protected health information (PHI), including, but not limited to cellular telephone use, email, computer password, information systems access, remote access, business

associates, record storage and security, final disposition of PHI and / or the electronic media on which it is stored.

After leaving their employment with HeliosDX, ex-employees must continue to protect the privacy of patients' health information. All departing employees must immediately return to their supervisor any and all documents and electronic media containing confidential protected health information. They must also take care never to disclose without proper authorization any protected health information that they may recall after leaving employment with HeliosDX.

Non-compliance with this policy and associated procedures is a serious matter and may result in civil and criminal actions in addition to internal disciplinary action that could lead to immediate dismissal from employment.

ANNUAL POLICY REVIEWS

PURPOSE:

HeliosDX wants to ensure that it meets applicable State and Federal Guidelines by reviewing its overall operations and policies annually.

POLICY:

The Board of Directors shall review the appropriateness of governing documents, board policies, bylaws, mission statement, HeliosDX policies and compliance with legislative mandates and applicable State and Federal Guidelines on an annual basis.

PROCEDURES:

The Board of Directors in collaboration with the Director of Administrative Services shall initiate an annual review of board policies, bylaws and mission statement.