LHC GROUP, INC.	BUSINESS ASSOCIATES AND AGREEMENTS
EFFECTIVE DATE: 04/14/2003	DIVISION: LHC ADMINISTRATIVE
REVISED DATE: 04/20/05, 12/21/08, 03/01/09, 10/01/13, 07/01/15, 1/1/2019	CHAPTER: HIPAA PRIVACY RULE
APPROVED BY: POLICY COMMITTEE	POLICY NUMBER: 13.1.001
	PAGE 1 OF 4

PURPOSE:

To implement reasonable and appropriate policies and procedures to comply with the Privacy and Security Rule regulations of the Health Insurance Portability and Accountability Act (HIPAA) regarding Business associate contracts or other arrangements.

To respect and assure the privacy and security of protected health information of our customers and employees, LHC Group and its member entities:

- identifies business associates; and,
- enter into business associate agreements; in accordance to the provisions of the HIPAA regulations

POLICY:

HIPAA regulations require that covered entities enter into written contracts or other arrangements with business associates. Health care providers are considered "covered entities" under HIPAA if they provide medical or health services under Medicare Part A or Part B and electronically transmit or receive health information. A covered entity may be a business associate of another covered entity. LHC Group is a covered entity.

A "business associate" is a person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of protected health information. Business associate functions or activities performed on behalf of a covered entity include claims processing, data analysis, utilization review, billing, transcription services, temporary staffing services, and software development/maintenance. Business associates may include clearinghouses, medical billing services, lawyers, transcription contractors or others who have access to protected health information.

LHC Group and its member entities will identify business associates and require said business associates to provide satisfactory assurances via written contract that they will maintain the confidentiality and security of the protected health information (PHI) including electronic protected health information, and only access, use, disclose, or transfer protected health information for the purposes for which it was provided.

LHC Group shall ensure that contracts or contract addendums with applicable business associates are signed before the business associate creates, receives, maintains, or transmits electronic protected health information on behalf of LHC Group or its agencies.

PROCEDURE:

Relationships or potential relationships with non-members of LHC Group's workforce will be reviewed by the Director of Privacy and Compliance, or other designated appropriate members of management, to determine if a Business Associate relationship exists as defined by HIPAA regulations.

Business associates will agree to:

1. comply with all obligations of a business associate under HIPAA
2. not use or disclose protected health information other than as needed to carry out the business associate's responsibilities to the Company
3. implement appropriate safeguards in accordance with HIPAA to prevent the use or disclosure of protected health information
4. to the extent that the business associate creates, receives, maintains or transmits electronic health information on behalf of the Company, to comply with the HIPAA security rule and implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the electronic health information
5. immediately report to the Company any unauthorized use or disclosure of protected health information, including breaches of unsecured protected health information and any security incident of which it becomes aware
6. mitigate to the extent practicable, any harmful effect of an unauthorized use or disclosure
7. enter into agreements with any agents or subcontractor that will create, receive, maintain or transmit protected health information on behalf of the business associate that require the same restrictions, terms and conditions required under the Business Associate Agreement with the Company
8. provide to the Company any requests for access or amendment to protected health information that it receives directly
9. document disclosures of protected health information as would be required by the Company to respond to an individual's request for an accounting of disclosures and provide to the Company an accounting of disclosures if requested by the Company
10. make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity available to the HHS Secretary for purposes of determining the covered entity's compliance
11. agree that known violations of a material term of the contract or contract addendum may result in termination of the business associate relationship.

LHC Group will utilize two (2) formats for the Business Associate Agreement:

- The Business Associate Agreement form is a complete, free standing agreement between LHC Group and a Business Associate. This agreement will be used when no other contract exists; and,
- The Business Associate Addendum form can be used as an addendum to an underlying contract between the business associate and LHC Group.

LHC Group's HIPAA Director of Privacy and Compliance will ensure that any complaints received regarding privacy violations on the part of a business associate are reviewed and will advise the appropriate administrative staff regarding the appropriate course of action

LHC Group's Director of Privacy and Compliance, or other designated members of management will guide the appropriate return or destruction of the protected health information used, created or obtained by the business associate upon contract terminations.

PURPOSE:

To establish and document compliance with:

- HIPAA Privacy and Security Rule requirements in regards to computer system use and security;
- Applicable Sarbanes-Oxley Information Technology control standards.

To further establish acceptable use standards regarding LHC Group information systems and data to avoid exposure to various risks including but not limited to impact to our brand image, hacking attacks, compromise of network systems and services, and legal violations caused by inappropriate use. To define standards, procedures, and restrictions for users of mobile devices who have legitimate and approved business uses for connecting a mobile device to LHC Group's company network and data.

The goal of this policy is to protect the integrity of the confidential client, patient and business data that resides within LHC Group's technology infrastructure ("confidential information"). This policy is intended to prevent confidential information from being deliberately or inadvertently stored on an unsecured mobile device or carried over an insecure network where it could be accessed by unsanctioned resources. Therefore, no PII/PHI may be stored on any non LHC managed equipment. A breach of this type could result in loss of information, damage to critical applications, loss of revenue, potential legal violations, and damage to the company's public image. Therefore, all users using LHC Group's information systems and employing a desktop or mobile device connected to LHC Group's network, and/or which is capable of backing up, storing, or otherwise accessing confidential information or company data of any type, must adhere to this policy.

DEFINITIONS:

CONFIDENTIAL – means data or information is not made available or disclosed to unauthorized persons or processes.

ELECTRONIC PROTECTED HEALTH INFORMATION (EPHI) – means individually identifiable health information (IIHI) that is transmitted by electronic media or maintained in electronic media.

PROPRIETARY – means data or information that is exclusively owned by a private individual or corporation.

PROTECTED HEALTH INFORMATION (PHI) – means individually identifiable health information (IIHI) that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or media. IIHI means information that is a subset of health information, including demographic information collected from an individual and is created or received by a health care provider, health plan, employer or health care clearinghouse. Such

information relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual that identifies the individual with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

POLICY:

This policy applies to all:

1. LHC Group employees, contractors, consultants, temporary workers, third-party business associate employees, students, and others who are members of our workforce (referred to hereafter as "users");
2. Information systems and data owned or leased by LHC Group, or are otherwise connected to, stored on, or accessed by our computer systems, or computer networks; and
3. All devices and accompanying media that fit the following classifications:
    a. Smartphones
    b. Tablets
    c. Portable media devices
    d. Laptop/notebook/Ultrabook computers
    e. Any other electronic device capable of storing data and/or connecting to a network

    (individually a "mobile device" or collectively "mobile devices").

For purposes of this Policy, LHC considers a workstation to be any electronic device, such as a laptop, desktop computer, tablet, printer, network, phone, transmission media or other associated equipment, or any other device that performs similar functions, and electronic media stored in its immediate environment.

LHC Group is committed to protecting itself, its patients, users, and business partners from damaging or illegal actions caused by users of our information systems and data. Employees play an active role and are responsible for maintaining the security of LHC's computer resources under their control, and for protecting the integrity and privacy of the data maintained on these resources. There is no expectation of privacy when using LHC's electronic devices/transmission media (technical environment).

LHC Group information systems that store or provide access to electronic protected health information or sensitive financial information must be used and safeguarded in a manner that maximizes security and prevents unauthorized access.

All devices used to conduct LHC Group business must be used appropriately, responsibly, ethically, and in accordance with this policy. Unless otherwise approved in writing by LHC Group's Chief Information Officer, the use of all LHC Group-owned mobile devices will be centrally managed by LHC Group's IT department and will be enrolled in LHC's Mobile Device

Management system or joined to the LHC Group domain. Violations of this policy may result in disciplinary action, up to and including termination.

It is the responsibility of all users to read and understand this policy and to conduct their activities accordingly.

All users shall follow all LHC Group policies and procedures, which are designed to:

1. Specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstations that can access electronic protected information; and,
2. Establish physical safeguards for all workstations that access electronic protected information and restricting access to authorized users.

PROCEDURE:

General Use and Operations

All information systems are intended for business purposes only.

The Chief Information Officer (CIO), or appropriate designee, must approve all workstations (computers, tablets, etc.), software, systems, networks, and network connections prior to installation. Maintenance, modifications, uninstalls, and disposal is handled by Information Technology department staff or by contractors, consultants, vendors or other third parties that have been approved by the CIO or designee.

All users' personal e-mail and Internet use should be limited and must not interfere with the timely completion of work assignments, cause the depletion of computer supplies, cause degradation to the performance of the network, damage computer equipment, or otherwise violate LHC Group policies.

All users will have a unique ID for all information systems used for business purposes. System level and user level passwords must comply with the Password Management Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

Accessing data, a server, medical record or an account, for any purposes other than conducting LHC business, even if you have authorized access, is prohibited.

All systems will be maintained in accordance with our Information Systems Change Management Policy (13.2.011). Information systems hardware, software, and data may not be removed from Company premises unless such activity is due to a legitimate business need and is specifically authorized by the CIO or designee. This restriction does not apply to portable computing devices such as laptop computers and mobile devices that have been previously authorized by the CIO.

Confidential and Proprietary Information

LHC Group's confidential and proprietary information includes, but is not limited to: company, customer, vendor, or contractor information; personnel records; financial data; corporate strategies; competitor analysis information; trade secrets; property and service specifications; price lists, research data; customer lists; customer email addresses; customer mailing or street addresses; and customer or company credit card numbers.

This definition applies to all forms of communication, including, but not limited to, verbal, written, and electronic communication.

All LHC Group information systems users shall:

1. Participate in ongoing security training to prevent unauthorized access to confidential and proprietary information;
2. Not provide confidential or proprietary company information, knowingly or unknowingly, to parties outside of LHC Group in violation of confidentiality agreements or any applicable laws or regulations, including the SEC regulations that govern publicly traded companies; and,
3. Store data in the user's Company-provided folder on a designated network drive to assure that it is backed up and available for restoration in the event user's information is altered, damaged or deleted.
4. Be advised that LHC Group reserves the right to monitor their system activities, with or without user knowledge. There is no expectation of privacy when using LHC's electronic devices/transmission media (Technical environment).

Protecting the Rights of Others

All LHC Group information systems users shall:

1. Be cordial and professional with their electronic communications;
2. Not create or distribute any disruptive or offensive messages, including offensive comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin;
3. Report to their manager, supervisor, or the Help Desk, any documents, emails, or other forms of communication that contain objectionable content; and,
4. Not download, copy or distribute copyrighted documents, software, music, video, images or other legally protected works without the express permission of the owner or copyright holder.

Electronic Devices, Transmission Media or Associated Equipment

LHC Group:

1. Reserves the right to refuse access to the LHC Group Network or connected infrastructure, if such equipment is being used in a way that puts the company's systems, data, users, and clients at risk; *May revoke access to electronic devices, transmission media or associated equipment at any time and for any reason*.
2. Reserves the right to utilize Internet filtering software that is designed to identify and block access to Internet sites containing obscene and inappropriate material, as well as to other Internet sites that do not appear to have legitimate business value;
3. Does not guarantee that filtering software when used will block all obscene and inappropriate material, or that it will allow access to all sites that have legitimate business value; and
4. Provide an exception process for legitimate business purposes.

All LHC Group information systems users shall:

1. Use electronic devices, transmission media or associated equipment where such use is suitable for business purposes;
2. Use electronic devices, transmission media or associated equipment in a manner that is consistent with the Company's standards of business conduct and is part of the normal execution of an employee's job responsibilities;
3. Ensure that when transporting portable computing devices, the device will be locked, placed in a container/bag prior to exiting home or building, place container in trunk of vehicle or locked glove compartment. If no trunk or locked glove compartment, transport on backseat floorboard out of sight, keep vehicle locked and secured at all times and never leave device in the car overnight.
4. Comply with LHC Group policies, including this Acceptable Use Policy;
5. Not interfere with the security or effectiveness of any computer system;
6. Not utilize electronic devices, transmission media or associated equipment in a manner that negatively affect the user's job performance;
7. Not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of LHC Group or any unit of the LHC Group unless appropriately authorized to do so;
8. Not include explicit disclaimers unless it is clear from the context that the author is not representing LHC Group (example: "the opinions expressed are my own, and not those of my employer");
9. Not send excessively large emails or attachments. (If you encounter a problem contact the Help Desk for assistance.)
10. Exercise extreme caution in using email to communicate confidential or sensitive matters (see the above definitions);

11. Encrypt files that contain confidential and sensitive matters before sending outbound communication with such information to authorized non-LHC recipients. Contact LHC's Cyber Security Manager for guidance if needed;
12. Texting of PHI is prohibited on company issued and personal mobile devices in an effort to mitigate risk of breach of protected health information.
13. Taking pictures of patients, patient's wounds, patient's information or patient's location is prohibited on personal devices.
14. If using work device, pictures of patients, patient's wounds, patient's information or patient's location must be uploaded into the medical record and removed from the device within 72 hours.
15. Not send or forward, via e-mail, text or otherwise, information that contains confidential or sensitive information to the user's home computer or personal (non-LHC Group) e-mail account;
16. Not pose as anyone other than themselves when sending email, except when authorized to send messages for another and the email includes a statement indicating who is actually sending the e-mail;
17. Not send unsolicited email messages, including the sending of "junk mail", spam, or other material to individuals who did not specifically request such material.

Privacy

Company email and Internet records and data are subject to disclosure to law enforcement, government officials, and to other third parties through subpoena or other processes.

LHC Group:

1. Will provide appropriate access for our users;
2. Will routinely monitor email, internet activity, files and data stored or transmitted on electronic devices, transmission media or associated equipment;
3. With management approval, will access and review email, web sites, server logs and electronic files and any computer or electronic device connected the LHC Group network, should there be a reason to do so (for examples, suspected or reported policy breaches, suspected breaches of any law, statute, regulation, or court order). See also Requests for Remote Access and Monitoring policy (13.2.022.)
4. Reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

All LHC Group information systems users shall:

1. Always be aware that the data they create or store on computer systems remains company property;
2. Waive any right of privacy in anything they create, store, send or receive using LHC Group information systems;

3. Ensure that the business information contained in these messages is accurate, appropriate, and lawful;
4. Consent, by virtue of their usage, to allow Information Systems Department staff and other appropriate personnel to access and review email, web sites, server logs and electronic files and any computer or electronic device connected to the LHC Group network; and
5. Access, use or share LHC proprietary information only to the extent it is authorized and necessary to fulfill assigned job duties.

Protecting Computer Systems and Data

All LHC Group information systems users shall:

1. Not provide any non-authorized user with access information or permit such persons use of LHC Group information systems;
2. Not circumvent security features of any computer or network system;
3. Protect information systems from unauthorized modification, duplication and from intentional and accidental damage or destruction;
4. Not purposely introduce malicious programs (e.g., viruses, worms, Trojan horses, spyware, etc.) into information systems;
5. Exercise extreme caution when downloading files from the Internet, opening email attachments, or using CDs, DVDs, USB drives and other storage media from non-company sources;
6. Delete any suspicious message that is received from someone that they do not know;
7. Report via "Spam Reports" or LHC Help Desk suspicious e-mails or email attachments, suspected viruses or malicious software;
8. Not enter information into a database, document, or computer file that is known to be false and/or unauthorized;
9. Not install any unauthorized app, software, computer program or device on LHC's network;
10. Not perform port scanning or security scanning as it is expressly prohibited unless prior notification to the Cyber Security Manager is made;
11. Not execute any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is part of the employee's normal job/duty;
12. Refrain from introducing honeypots, honeynets, or similar technology on LHC's network; and
13. Not use any program/script/command, or send messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

For any exceptions to the above, prior approval must be obtained from the Cyber Security Manager and/or the Chief Information Officer (CIO) via ticket request through the Help Desk.

Mobile Devices

Mobile Device Users should only connect to known networks and should exercise caution when connecting to non-LHC Group networks. (for example, users should avoid unknown open Wi-Fi connections) When connecting to open networks at hotels, restaurants, etc. all users should connect to the LHC VPN.

Mobile Device Management ("MDM")

1. LHC Group uses an MDM system to secure mobile devices and to enforce policies remotely. Before connecting a mobile device to LHC Group networks of any kind, the mobile device must be enrolled in this system.
2. The MDM client application must be installed on all mobile devices connecting to company resources.
3. Any attempt to contravene or bypass the MDM system will result in immediate disconnection from all company resources and may result in disciplinary action up to and including termination of employment.
4. All MDM managed devices must be turned on and connected to the internet at least every 30 days to check into the MDM. For any device that is not checked in with MDM after 30 days, access will be suspended from the system.
5. All MDM managed devices will be required to have a cellular data plan.

Mobile Device Security

1. All mobile devices must adhere to the Password Management Policy. Employees must never disclose their passwords/PIN to anyone.
2. All users of mobile devices must employ reasonable physical security measures. Users are expected to secure all such devices against being lost or stolen, whether or not they are actually in use or being carried.
3. Passwords are not to be stored on or attached to mobile devices (for example, with sticky notes or in computer).
4. In the event a workstation device is lost or stolen, see Security Incident Reporting and Response policy. You have the responsibility to promptly report the theft, loss or unauthorized disclosure of proprietary information or devices, see Lost/Stolen Device Process/Form.

Mobile Device Hardware & Support

1. LHC Group reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the enterprise network or connected infrastructure and devices.

2. Users will make no modifications to the hardware or software that change the nature of the device (e.g. replacing or overriding the operating system, jail breaking, rooting).
3. IT will support the connection of mobile devices to company resources on company issued devices. IT will **not** be responsible for non-LHC devices, networks, or non-company applications.

Workstation Security

For workstations located in restricted areas where access to the space is restricted to employees or LHC contractors, and guests are typically announced/escorted into such areas:

1. Access to the workstation will require a Company issued user id and password.
2. When walking away from their workstations, employees must lock the workstation or log off.

For workstations located in restricted areas with a higher probability of non-employees, such as family members, being present (for example, an LTACH floor or hospice inpatient unit) and Company workforce members are usually present in the vicinity of the workstations:

1. Workstations must be oriented so that the screens are not easily visible to a guest.
2. If needed, security screens should be used to limit the ability of a guest to view the screen.
3. If a determination is made that there is a high risk of loss, then the workstation will be physically secured using a locking device, or a cable with a locking device.

For workstations that are located in settings other than an LHC Group facility (for example: those used by work at home employees):

1. The employee must ensure that no-one else accesses, or attempts to access, the workstation.
2. Access to the workstation will require a Company issued user id and password.

Employees with mobile workstations (laptop computers/tablet devices) must:

1. Exercise reasonable efforts to keep the device in a secure location when not in use
2. Not leave the device unattended
3. Use reasonable judgment when using the device in spaces where there is a potential for someone to "peek" and take one of the following actions as appropriate:
    a. Use a privacy screen (which can be procured by contacting the IT department)
    b. Angle the screen so that content is not visible
    c. Not use the workstation
4. Not allow un-authorized users to use the workstation.

In the event a workstation device is lost or stolen, see Security Incident Reporting and Response policy (13.2.025). You have the responsibility to promptly report the theft, loss or unauthorized disclosure of proprietary information or devices, see Lost/Stolen Device Process/Form.

Users must **immediately report** to his/her manager **and** the Cyber Security Manager **any incident or suspected incidents of unauthorized data access**, data loss, and/or disclosure of company resources, databases, networks, etc.

LHC Group will NOT reimburse employees if they choose to purchase their own mobile devices. Users of their own devices will NOT be allowed to expense mobile network usage costs.
Use of personal electronic devices (devices not issued by LHC Group) to access protected information is prohibited unless otherwise authorized.

Failure to comply with this policy and procedure may result in disciplinary action up to, and including, termination from the Company's workforce.

See also Facility Access Controls policy.