Information Technology (IT) Department

Policies and Procedures

Our MISSION: To Improve the Health of the People We Serve.

Our VISION: To Exceed National Performance Standards for Quality Care and to Improve Access for Patients through Expanded Medical Services and New Sites.

Access Health Louisiana
2900 Indiana Ave
Kenner, LA 70065

Signature:_____

Date: _____

I have read, understand, and agree to follow all policies and procedures within this manual.

Approved by the Board of Directors:
Implementation:

Information Technology Department(ITD)

Policies and Procedures

Our MISSION: To Improve the Health of the People We Serve.

Our VISION: To Exceed National Performance Standards for Quality Care and to Improve Access for Patients through Expanded Medical Services and New Sites.

Approved by the Board of Directors:
Implementation:

The purpose of this manual is to detail all the policies and procedures pertaining to the Information Technology (IT) Department of Access Health Louisiana (AHL).

This manual is divided into distinct sections and organized by a decimal system. For example, Section 100 is "Access Health Louisiana Information Management Policies and Procedures: Introduction and Manual Organization"; next is section 101, "Access Health Louisiana Information Technology Department". Section 200 begins with "HIPAA and PHI".

SECTION 100 Information Management Policies and Procedures Introduction and Manual Organization

Policy: **IT-100.1**: The Information Technology Policies and Procedures will be reviewed on an annual basis.

Policy: **IT-100.2**: Initially each Management Information System (MIS) user will receive a paper copy of the Information Technology Departments Policies and Procedures.

- You may request additional paper copies of the Policies and Procedures document through IT Department by putting in a help ticket at helpdesk@acceshealthla.org.

Policy: **IT-100.3**: A copy of the Information Technology Departments Policies and Procedures manual will be available on the Intranet. (SharePoint)

- The IT Policies and Procedures can be found online by going to https://sp02/sitepages/home.aspx. (Internal Access) Or https://sharepoint.accesshealthla.org (External)

Policy: **IT-100.4**: The Information Technology (IT) staff can bypass or make an exception to any Management Information System (MIS) procedure to resolve problems in an emergency situation or if they diagnose the system as being down.

SECTION 101 Information Technology

Access Health Louisiana Information Technology (IT) Department over sees the management of Information Architecture, data integrity, integration design, security, connectivity, support and training with specialized data bases and provides maintenance, application support, general training and reporting.

Per HIPAA legislation, Access Health Louisiana is required to have an active Security Officer. This Security Officer is the IT Manager of the Information Technology Department.

Policy: **IT-101.1**: Information Technology.

Access Health Louisiana IT Department, in its broadest use, is defined as any equipment, network operating systems, site to site location, applications, data, Protected Health Information (PHI), and any other equipment or data that makes up Access Health Louisiana's Information Systems. Its definition also includes any functionality or integration of itself.

Access Health Louisiana IT Department's purpose is to collect, organize, store, maintain, secure, and present data in schemes to reflect the methodology and diverseness of the organizational values. In doing this effectively, AHL's IT Department will streamline and enhance the capture and flow of AHL's data, information and knowledge and deliver it to individuals and groups engaged in accomplishing work. Further, it will embrace a diversity of knowledge sources to include databases, web-sites, AHL users, and partners, through relating that knowledge where it resides, while at the same time capturing its content and giving it greater meaning through its relation to other information in the organization.

AHL's IT Department as of 2016 is a multiple platform computer system that is built off of a variety of information systems

A description of the INFORMATION SYSTEMS are listed below:

1. State of the act Data Center (Venyu)
2. ESI VMWare Server Ver. 5.5 -6
3. Window Server 2003-2012
4. Linux PBX Phone Server ver. 12
5. Cisco Meraki MX64 & MX84 Routers
6. HP Switches
7. Veeam Backup & Replication Enterprise Plus
8. Solar Winds
9. Barracuda Firewall
10. Cisco AnyConnect
11. Microsoft Office 365

12. Exchange mail Server
13. Window OS 7 & 10
14. Desktop Window 7
15. Laptop Window 7
16. Surface Window 10
17. Circuit Fiber and Coax
18. Intrusion Prevention System (IPS)
19. Intrusion detection System (IDS)
20. Netapps Storage (3) Server (NAS)
21. Cisco Phone VOIP
22. Alarm systems with Camera's

SECTION 200 The Health Information Portability and Accountability Act and Protected Health Information (PHI)

I. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was signed into law on August 21, 1996 (P.L.104-196). It contains a broad spectrum of legislation that focuses on the following three areas:

- Insurance Portability
- Fraud Enforcement
- Administrative Simplification

Insurance Portability and Fraud Enforcement are non-applicable to Information Management Policies and Procedures. Thus, they will not be covered in this manual. The policies and procedures in this section deal only with the security component of HIPAA.

The Administrative Simplification component of the HIPAA legislation implements regulations for standardizing electronic transactions of health care data. It also contains provisions for the Privacy and Security of personal health information. Administrative Simplification applies to all maintained and transmitted forms of personal health information – including paper, electronic, or oral communications.

II. Protected Health Information (PHI) is defined as any individually identifiable health information that is transmitted or maintained in any form or medium by an entity covered under HIPAA. Basically, this means that any information that would go in the patient's medical record or chart that could be used to identify the patient from a list of other patients with similar information should be considered PHI.

Examples Patient **Protected Health Information** includes the following:

- Name
- Street Address
- City
- Country
- Precinct
- Zip Codes
- Names of Relatives and employers
- Date of Birth
- Date of Service
- Telephone number
- Web URL and IP Address
- Biometrics (finger prints, voice prints, iris scan, etc.)
- Fax number
- E-mail address
- Social Security Number
- Medical Record Number
- Health Plan Beneficiary Number
- Account and Chart Numbers
- Certificate / License Numbers
- Vehicle Identification
- Device Identifiers
- Photographs
- And any other unique identifying number, characteristic, or code (whether generally available to the public realm or not)

There are seven basic provisions governing use of PHI:

1. PHI may be used by AHL for purposes of treatment, billing, or operations related to treatment and billing with or without patient consent.
2. AHL is required to notify all patients of how PHI is used and to ask all patients for consent to use PHI for any reason (even treatment and billing), but if consent is not granted by the patient, PHI can be used for treatment and billing operations without patient consent.
3. AHL is required to obtain patient consent for using PHI for any other reason including marketing, fund raising or solicitation for research studies.
4. AHL is required to obtain authorization from the patient prior to release or disclosure of PHI to the patient's designee or other entities.
5. If information is being disclosed, AHL will make an effort to disclose only the minimum amount of information necessary to meet the needs of the individual or entity requesting the information.
6. AHL is required to De-identify information that will be used for other purposes if consent has not been granted by the patient.
7. AHL is required to obtain agreements with any Business Associates who receive PHI that bind the Business Associate to comply with AHL's information practices policies.

Policy: **IT-200.1**: Access Health Louisiana will establish methodologies for monitoring activities related to the privacy and security of protected health information. AHL will audit activities related to the privacy and security of protected health information at regular intervals throughout the year.

A. Access Health Louisiana will monitor the following:
    - Use, disclosure and release of protected health information
    - Access to system and medical records
    - System maintenance activities
    - Document storage and disposal activities
    - Records of each time information is accessed
    - Records of system maintenance activities
    - Records of document storage
    - Hardware and software inventories

Policy: **IT-200.2**: From time to time, patients will ask that AHL receive transfers of their PHI electronically from other providers or payers. Access health Louisiana will make every effort to ensure that the electronic transfer occurs in a secure fashion and that records are maintained securely.

A. Routine and non-routine transfers of patient information will be treated with the same standards as current electronic medical records are treated.
B. The practice will develop a methodology along with its vendor for the receipt, transmission and dissemination of electronic health information.

Policy: **IT-200.3**: All data transactions that occur through third parties (e.g.: claims clearinghouses or billing agencies) will be subject to the signature of a chain of trust agreement with those parties before data can be transacted or disclosed.

A. AHL's attorneys will develop a "chain of trust" contract for the practice and its third-party contractors. This is a contract in which the parties agree to electronically transmit data and protect the transmitted data in ways compliant with HIPAA security standards.
B. All third-party contractors to whom protected health information is transmitted electronically will be required to sign chain of trust agreements. This agreement does not include referring physicians or hospitals that use data for the treatment or billing for treatment of the patient.
C. Contracts will be kept on file in central files. Contracts will be reviewed every three years along with other administrative safeguards.
D. Once a year, in order to monitor compliance with the agreement, the security officer of AHL will contact all chain of trust partners of the practice and ask them to confirm that data being transmitted is secure and that their data practices are HIPAA compliant. Confirmation could include obtaining copies of certification of security practices of the chain of trust partner but it will be left to the discretion of the AHL security officer to determine sufficient compliance with the chain of trust agreement.

Policy: **IT-200.4**: Access Health Louisiana will take reasonable steps to limit the use of disclosure of Protected Health Information.

This policy does not apply to disclosure requests from referring physicians or health care providers who are treating the patient, the individual who is the subject of the information, standard HIPAA transactions, Department of Health and Human Services (DHHS), and law enforcement officials and other uses or disclosures required by law.

A. Access to protected health information and the type of information available will be limited to the AHL users who need the information to conduct their work duties. The security plan contains a list of AHL user job descriptions and levels of access to information.
B. Routine or recurring requests from payers (for example: requests for chart notes or prepayment reviews) will have limited information released and it will be restricted to the service in question.
C. Non-routine requests will be handled by requiring the releasing party to use the following criteria to determine the amount of information that needs to be released:
    - Is the information required to support a claim or receive payment?
    - If information is not released, will it delay quick, effective treatment?
    - Is releasing the information consistent with professional standards of protecting the unnecessary sharing of patient information?

D. The judgment of the party requesting the information may be relied upon to determine the minimum amount of information necessary for its purpose, in certain circumstances. If the request for information is made by a public official or agency, another provider or representative from a payer or a medical researcher, with appropriate documentation from an Institutional Review Board must be provided, then the exact information being requested, can be released to them.
E. Any information released in this manner will be subject to verification of the identity of the person requesting the information. Identity can be verified by asking for written requests on company letterhead or request in person with appropriate corporate identification.

Policy: **IT-200.5**: All Protected Health Information being used for any purpose other than treatment, billing or operations related to treatment and billing, the information will be "de-identified" by removing all information that could distinguish the individual's record from a group of records.

A. The patient's name, address, diagnosis, chart notes, lab results, treatment plan, insurance or financial information are all considered protected health information. All of these elements appearing together could be used to identify a patient.
B. The AHL manager will have the responsibility of determining the information on a report that could reasonably be used to identify an individual.
C. Any information that can uniquely identify the patient will be removed from data printouts or reports. (For example: a report to analyze treatment patterns by market could contain zip codes and diagnoses but not patient address or names)
D. Patient address information can be used for newsletters and for contacting the patient prior to an appointment but will not be used for targeted marketing activities. (For example: the practice could send out quarterly newsletters to its entire patient base but the practice could not develop and send marketing materials to patients who have had a specific treatment plan for a hip injury, unless the patients indicate that they would like to receive such targeted materials on their consent forms)

Policy: **IT-200.6**: Any Access Health Louisiana user who attempts to bypass such practices as outlined in policies IT-200.1 through IT-200.5 will be subject to disciplinary action up to and including possible termination of employment. In the case of a non-employed AHL user, access to AHL will be locked- out.

SECTION 300 Access Health Louisiana Users: Creations of Accounts, Training and Terminations

To insure a proper understanding of computer and security policies and procedures AHL is requiring all AHL users to attend various computer use, application use, and security training sessions.

A. Computer Use Training – This will cover general training on general PC and Laptop use, Windows use, and other Network Operating System services. This will also cover training on acceptable PC and Laptop use.

B. Application Use Training – This will cover training on the applications that will be made available for the AHL user by the AHL Information Technology Department. The AHL user will also be trained on the proper method / methods of communicating new requests and system problems to the Information Technology Department.

C. Security Training – This will cover training on Computer, Email, and Internet Security. The Access Health user will also be trained on acceptable PC and Laptop use as it pertains to security.

Policy: **IT-300.1**: AHL users must fall within one of the following AHL user categories to be given access to AHL. (1) Any authorized employee type as defined in the Access Health Louisiana Human Resources Manual. (2) Board members, unless an exception is made by the IT department in conjunction with the Director of Human Resources.

Policy: **IT-300.2**: AHL is requiring all AHL users and consultants to sign an agreement of confidentiality to prevent unauthorized disclosure of sensitive business and technical information including but not limited to work in progress, work planned concepts, know-how and trade secrets specifically relating to health care and health care information systems.

A. Employees. As a condition of employment, Access Health Louisiana will require all employees to sign a separate document entitled Access Health Louisiana Confidentiality Agreement. The term "Employee" refers to all full and part-time employees including but not limited to: temporary, contract, volunteer, and student personnel.
B. Information Management and Telephony Consultants. All external Telephony and Information Systems Consultants may be required to sign a separate document entitled Access Health Louisiana Confidentiality Agreement. The term "Telephony and Information Systems Consultants" includes but is not limited to integrators, programmers, hardware and software technicians, telephone system technicians, and Internet carriers, with the exception of circuit providers. The Chief Executive Officer (CEO) or designee may waive this requirement on a vendor by vendor basis.

C. Financial and Business Consultants. All external Financial and Business Consultants who have the possibility of coming in to contact with any technical, strategic, and marketing plans, financial reports, projections, production figures, capacities, detailed technical information and processes, business and financial information on contracts, supply arrangements, patient volumes, clinical and demographic patient information, information contained in tax returns, or financial statements may be required to sign a separate document entitled Access Health Louisiana Confidentiality Agreement. The term "Financial and Business Consultants" includes but is not limited to grant, marketing, strategic, and special project consultants, attorneys, auditors, or any other agency or person that comes into contact with any of the aforementioned information. The Chief Executive Officer (CEO) or designee may waive this requirement on a consultant by consultant basis.

Policy: **IT-300.3**: An Employee Action Communication Form must be completed by the AHL user's supervisor, before a AHL user account can be created for an authorized full or part time employee, temporary employee, contractor, volunteer, student, board member or other personnel

- There is a two-day timeframe for each AHL user account creation. Insure the form is completed at least 2 days before the action date.
- You can find this form by going to http://sharepoint.accesshealthla.org website

Policy: **IT-300.4**: AHL will require all users to attend initial computer use, application use, and security training sessions before receiving access codes or passwords to AHL. The users will include, but not limited to, any authorized full or part time employee, temporary employee, contract volunteer, student, board member or other personnel accessing AHL from either an external or internal console

Policy: **IT-300.5**: New or Current AHL users are required to complete AHL training.

A. All AHL users will be required to attend compliance training when offered. To signify completion of training, all participants must complete a post-test and sign the attestation of attendance and compliance agreement. (ex. Sign on the computer and print).
B. All new AHL users will be required to complete the security training sessions within fifteen (15) days of employment. To signify completion of training, all participants must complete the post-test and sign the attestation of completion and compliance agreement.
C. Compliance training will be ongoing and continued participation is required. Training may occur in staff meetings, via newsletters, e-mails, bulletin boards, or online.

Policy: **IT-300.6**: IT Department must be directly notified by Supervisors, 24 hours before a AHL user's planned termination or resignation. In the case of an unplanned termination, IT must be directly notified by the end of the day that the termination takes place. An Employee Action Communication form will have to be completed to communicate this termination. Furthermore, it is the responsibility of IT to disable or lockout access to AHL.

- You can find this form by going to http://sharepoint.accesshealthla.org website

Access Health Louisiana has implemented Virtual Private Networking (VPN) or remote access to allow AHL users to connect to AHL from AHL authorized computer.

Policy: **IT-300.7**: Remote access and the installation and continuation of use of AHL owned software on a AHL user's home personal computer or laptop will be subject to a separate document entitled "Conditions for installation of Access Health Louisiana owned software on a privately owned computer".

Policy: **IT-300.8**: Any AHL user who participates or attempts to bypass such practices as outlined in policies 300.1 through 300.7 will be subject to disciplinary action up to and including possible termination of employment. In the case of a non-employed AHL user, access to AHL will be locked- out.

SECTION 400 Security and Risks: Access Health Louisiana Users

A. An AHL user is defined as any authorized full or part time employee, temporary employee, contract, volunteer, student, or board member accessing AHL from either an external or internal console.
B. User authentication security is defined as any measures utilized to accurately authenticate and identify authorized and unauthorized users of equipment, data, or network systems. It is also defined, for convenience within this manual, as any policy or procedure relating to authenticating and identifying authorized users.
C. AHL's User Authentication Security risks are passwords, user accounts, and any other method of accurately authenticating and identifying authorized users. An acceptable User Authentication Security design will prevent unauthorized access from a breach of security originating from easily guessed passwords, password or account sharing, and password or account hacking.
D. To prevent and counteract account password hacking or cracking, AHL automatically prompts users to change their password after a given duration of days (this process cannot be bypassed), further it will not allow users to change their password to one that has been used during the past several changes. AHL locks out an account after several inaccurate authentication attempts; this lockout exists for a given amount of time.

Policy: **IT-400.1**: AHL Systems have a password complexity requirement for all passwords used by AHL Users:

A. Passwords must be at least 10 characters long.
B. Passwords may not contain your AHL username, any part of your full name, birth date, or social security number. (ie: jsmith000 is not acceptable)
C. Passwords must contain characters from at least three of the following four categories:
    - Upper case letters (i.e.: A,B,C,…Z)
    - Lower case letters (i.e.: a,b,c,…z)
    - Numbers (i.e.: 0,1,2,…9)
    - Punctuation marks and other symbols (i.e.: !,@,#,$,%,…>, etc.)

Policy: **IT-400.2**: AHL Voicemail has a password complexity requirement for all passwords used by AHL users on all telephone voicemail systems (including office phone voicemail, cell phone voicemail, and all other voicemail telephony systems):

- Passwords must be at least 4 to 6 numerals long
- Passwords must not contain your telephone extension or any part of a Access Health Louisiana phone number.
- Passwords must not have more than 2 repeating numbers (i.e.: 1110 or 1111 are not acceptable) and must not have more than 2 numbers in consecutive order (i.e.: 1231, 1234 and 9876 are not acceptable.

Policy: **IT-400.3**: AHL automatically requires users to change their passwords every 60 days. AHL will prevent users from using their past 5 (five) passwords.

Policy: **IT-400.4**: AHL will implement systems that automatically lock AHL user sessions within a maximum 5-minute timeline of inactivity. If this timeline is seen to disrupt efficiency, some other type of authentication method will need to be implemented after evaluation (i.e.: proximity or biometrics).

Policy: **IT-400.5**: AHL will implement systems that prevent users from logging on after business hours and during weekends. Exceptions to the policy will only be given on an as needed basis.

- Requests for exceptions will need to be submitted to the IT department at least 2 days in advance, by the user's direct supervisor.

Policy: **IT-400.6**: AHL users who use Any Electronics devices that contain AHL information must password protect them when not in use.

Policy: **IT-400.7**: AHL has implemented systems that lockout accounts after a maximum of 3 (three) inaccurate authentication attempts. This lockout exists for a maximum duration of 1 (one) hour unless overridden by an IT staff member.

Policy: **IT-400.8**: Passwords that are used to access any AHL service, device, or computer, whether owned or not owned by Access Health Louisiana, that contains Access Health Louisiana data falls under the category of "confidential information" as defined in a separate document entitled Access Health Louisiana Confidentiality Agreement. As such, AHL users will not store any of their passwords in any way, other than through memorization. Inappropriate examples of storing passwords are recording a password in a personal notebook, wallet, purse, or posting a password on a monitor, under a keyboard, etc.

Policy: **IT-400.9**: AHL users will not divulge their authentication code or password to anyone, including their supervisor, unless requested by an IT staff member or with written permission from IT.

Policy: **IT-400.10**: AHL users will not divulge any *user name, password, PIN, building alarm code, or other secret code including but not limited to modem, telephone numbers and TCP/IP addresses* to any person over a telephone, cell phone, or other telephony device, unless prior approval has been granted (per each assistance) by the IT department. If any person calls and asks for any of the aforementioned information over a telephone, cellphone, or other telephony device the AHL user will refer them to call Access Health Louisiana Information Technology Department at (985)785-5800.

Policy: **IT-400.11**: All AHL Users are required to log off of terminals before leaving them unattended for any length of time. At no time is a AHL user allowed to log on using another AHL user's password.

Policy: **IT-400.12**: Patient, family members, patient representatives or AHL user family members are prohibited from viewing data in the system or gaining access to AHL Network Systems, under any circumstances.

Policy: **IT-400.13**: AHL users are prohibited from installing software on any AHL computer, workstation, server or device without expressed permission from an IT department staff member. The only users who are authorized to install software without permission are those employees within the IT Department. Software that was not authorized by the IT department, if found on a AHL owned computer, will immediately be uninstalled.

Policy: **IT-400.14**: AHL users are prohibited from installing and/or playing games on AHL technology devices.

Policy: **IT-400.15**: AHL users are prohibited from downloading applications or programs off of the Internet using AHL technology devices. Though it is noted however, the downloading of *data files* (i.e. PDF files, Word Processing Files, Sound Files, etc.) are not considered applications or programs within this manual.

Policy: **IT-400.16**: AHL users are prohibited from participating in the use of or installing of software to be used with file, movie, video, or music sharing networks. Examples of file, movie, video, and music sharing networks are Napster, Kazaa, and Morpheus. If file, movie, video, or music sharing software is found on a AHL owned computer – the software will immediately be uninstalled, unless authorized by the IT Manager.

Policy: **IT-400.17**: AHL users are prohibited from participating in the use of or installation of software to be used with any instant messaging or chat service, unless organizationally implemented as an IT service. For instant messaging to be implemented organizationally it must be proven to be secure and auditable. Examples of instant messaging and chat services are AOL Instant Messenger, MSN, ICQ, and IRC. If instant messaging or chat service software is found on a AHL owned computer – the software will immediately be uninstalled.

Policy: **IT-400.18**: AHL users are prohibited from the transport of AHL information using any free email service or any third party email account, unless otherwise approved by the IT Manager. Examples of free email services are Hotmail, Juno, Yahoo, etc. An example of a third party email account would be your personal home email. The only email

services that are available for the transmission of AHL information are email services provided to users by Access Health Louisiana' Information Technology department. If free or third party email access software is found on a AHL owned computer – the software will immediately be uninstalled.

Policy: **IT-400.19**: AHL users are prohibited from emailing or attaching to an email, any form of information containing a patient's Name, Address, Date of Birth, Date of Service, Telephone number, Fax number, E-mail address, Social Security Number, Account Number, Certificate / License Number, Vehicle Identification number, photograph, biometric information, or any other type of Protected Health Information.

Policy: **IT-400.20**: AHL users are prohibited from accessing, causing to be accessed, or creating the possibility of accessing any system, equipment, or data that they are not authorized to use.

Policy: **IT-400.21**: AHL users are prohibited from searching for, displaying, printing, creating, buying, selling or distribution of pornography, using any portion of AHL.

Policy: **IT-400.22**: AHL users are prohibited from the bypassing of proper identification by logging on to any AHL system as someone else. AHL users are not allowed to share accounts, in any form.

Policy: **IT-400.23**: Non-AHL users are prohibited from access to the AHL networking infrastructure.

A. Non-AHL users are defined as any person who does not have direct access to AHL or who does not have an individual AHL account. Examples of non-AHL users are Drug Reps, vendors, and janitorial staff.

Policy: **IT-400.24**: AHL are prohibited from installing or connecting any type of hardware to any portion of AHL unless written permission has been granted from the IT department.

Policy: **IT-400.25:** AHL users faxing out going documents must use a cover sheet that clearly details a security disclaimer. The cover sheet must not contain any type of Protected Health Information.

- AHL users will take care to insure faxed documents are only received by the intended recipient(s). Reasonable methods of insuring this are:
    - Double-checking fax numbers
    - Keeping a fax number "cheat sheet" near the fax machine
    - Calling the intended recipient to insure the fax arrived

AHL licenses the use of computer software from a variety of outside companies. AHL does not own this software or its related documentation and unless authorized by the software developer, does not have the right to reproduce it except for backup purposes. According to applicable copyright law, persons involved in the illegal reproduction of software can be subject to civil damages and criminal penalties.

Policy: **IT-400.26**: AHL users will use software only in accordance with the license agreements.

Policy: **IT-400.27**: AHL users learning of any misuse of software or related documentation are required to notify their supervisor or the IT department immediately.

Access Health Louisiana implemented a Helpdesk system to track AHL user's computer, telephone, cell phone, long-distance, and pager requests. This system was designed to make use of standardized incident subjects (i.e.: E-time, ADP, Medic, Telephone, and Time Clocks). Given the Service Level Agreement (SLA) or priority per each user, center, or standardized support subject, the system emails or messages IT personnel via their cell phones. Automatically based on the SLA is an expected resolution time frame. This resolution time can vary based on workflow and other projects.

Policy: **IT-400.28**: AHL users needing to communicate an incident or new request to the Information Technology Department will use the Helpdesk system.

A. Each new AHL user will receive an initial training on the proper use of the Helpdesk.
B. An AHL Helpdesk manual can be found online by going to https://Sharepoint.accesshealthla.org website.
C. AHL users may request a paper manual by entering an incident into the helpdesk system.
D. If the Helpdesk is unavailable due to a system problem, then please contact the IT Department by calling (985) 785-5859.
    - If no one answers your call will go to the next available technician

Policy: **IT-400.29**: Any AHL user who participates or attempts to bypass such practices as outlined in policies 301.1 through 301.28 will be subject to disciplinary action up to and including possible termination of employment. In the case of a non-employed AHL user, access to AHL will be locked- out.

SECTION 410 Security and Risks: Access Health Louisiana Users

AHL's Datacenter(Venyu) physical security risks are building security, server rooms, network equipment, and Wide Area Network (WAN) provider connectivity equipment. Physical security begins with locking server and network equipment room doors and having office security systems.

Policy: **IT-410.1**: Only employed AHL users shall receive keys, codes, or pass phrases to building alarm systems and perimeter door locks.

Policy: **IT-410.2**: AHL users having received keys, codes or pass phrases to building alarm systems and perimeter door locks will not bypass proper identification by swiping or coding in as someone else. AHL users are prohibited from sharing their building alarm system and perimeter door lock keys, codes, or pass phrases, in any form.

- In the event that an authorized person has forgotten their keys, codes, or pass phrases to a building alarm system or perimeter door lock – they are to use the public entrance.

Policy: **IT-410.3**: Employee only entrances or back door perimeter door locks must remain locked at all times.

Policy: **IT-410.4**: AHL will make every effort to ensure that there are physical safeguards in place to protect data from inadvertent or illegal access.

A. Receipt of any diskettes, tapes or other forms of media that contain Protected Health Information (PHI) will be noted in the AHL information management inventory. Information will be transferred to the practice system in a timely fashion (within 10 days) and materials used for transmission of information will be destroyed.
B. Removal of hardware and software from any AHL site that might contain protected health information is prohibited.
C. AHL will keep a log of system maintenance procedures and verify the identification of any maintenance personnel not known.
D. Workstations will be placed in secure areas where monitors are not easily viewed by patients or unauthorized personnel.
E. All visitors to the practice for reasons other than treatment will be asked to sign in and verify their identity before being allowed to enter secure areas.

Policy: **IT-410.5**: AHL as well as the Datacenter (Venyu) will physically secure all offices and rooms containing AHL owned servers, integral switching, routing and Wide Area Network provider connectivity equipment. In addition, AHL will also secure rooms containing corporate consolidated organizational data, information, and knowledge in the electronic form.

Policy: **IT-410.6**: Only those AHL users who require day to day access to the areas in policy 410.5 shall receive keys or codes to those secure places.

Policy: **IT-410.7**: Vendors, consultants, and service providers shall not receive keys or codes to sensitive equipment or data storage areas, without approval from the Manager (IT) or Designee.

Policy: **IT-410.8:** AHL equipment and devices must be positioned within offices such that information cannot be seen by non-AHL users.

- AHL equipment and devices include but are not limited to computers, monitors, fax machines, copiers, printers, scanners or any other equipment or devices that contain, display, or capture AHL Information.

Policy: **IT-410.9**: All personnel will wear their name tag and / or photo ID at all times while on any company premises.

Policy: **IT-410.10**: Any AHL user who participates or attempts to bypass such practices as outlined in policies 410.1 through 410.9 will be subject to disciplinary action up to and including possible termination of employment. In the case of a non-employed AHL user, access will be locked-out.

SECTION 500 Access Health Louisiana Information Technology Departmental Security Policies

Network Operating System (NOS) Security is the biggest determining factor of AHL's security. A NOS is any Operating System (OS) that is network aware. A network is a method of connecting multiple systems together to achieve something greater than its part. An OS is any software system that primarily operates a computer. Windows NT Server and Workstation or Windows 2003-2012 and Linux Server and Professional is a NOS, while natively Windows 7, and 10 have very little built in security, short of integrating with a Windows 2003-2012 Server. A network can be made up of multiple NOS. Using this cross-platform architecture creates diversity in what and how information can be accessed and integrated. Cross-platform architecture is the method of integrating multiple NOS and applications into a seamless system (i.e.: Multiview 2003, Linux and ESI Server with VMWare).

AHL's NOS risks are file, directory, and service (i.e.: Internet Firewall) authentication. A secure NOS will protect and prevent internal and external factors from causing data loss, data damage, and unauthorized access. To fully secure an integrated network each part needs to be secured individually – as well as the whole. Each NOS part, from data management to presentation, has to authenticate legitimate users beginning with password level.

AHL's primary NOS are Windows 2000, AIX, and Linux. AHL: uses Microsoft Windows object and auditing security services. Firewalls provide Internet security on AHL's internal network and a virus shielding server provides scanning of Web, FTP, POP, and SMTP packets.

Connectivity Security is the security implemented on the transport, data link, and connection portions of a network that prevent unauthorized individuals from interrupting or intercepting data in transport. It also prevents unauthorized users from connecting to or accessing services, devices, and data. *Physical Security* is the physical barriers that prevent unauthorized individuals from gaining access to integral equipment.

AHL's Connectivity risks are Internet access, Virtual Private Networking (VPN), dial-up, telephone, and Physical Network Link Access. An acceptable connectivity security design will prevent unauthorized access to internal services, equipment, and data originating from a breach in the internal security services of Firewall, VPN, dial-up, telephone, and Physical Network Link Access.

AHL uses Cisco/HP switches and routers to facilitate AHL connectivity. Routers and switches are monitored with Solar Winds. Connectivity between sites is achieved through the use of dedicated point to point T1, Coax and Fiber lines. Unused switch ports are disabled to prevent unauthorized network access. Switches and Routers are password protected. A Barracuda firewall and IDS/IPS is used to protect AHL from Internet attacks. Log entries are generated on a per hit basis. Possible unauthorized Internet penetration is logged. Daily reports are available to authorized personnel.

Policy: **IT-500.1**: AHL will only integrate applications, network operating systems, and technological services that are considered by industry standards to be secure. Those aforementioned integrated components must also be capable of preventing internal and external factors from causing data loss, data damage, and unauthorized access.

Policy: **IT-500.2**: AHL's administrator passwords will be changed with in 24 hrs. in the event of Senior Management or Information Technology Department personnel changes.

Policy: **IT-500.3**: Access Health Louisiana will manage system integrity by proactively checking for viruses, detecting and containing inadvertent or illegal access, developing an inventory of all hardware and software and correction of any weaknesses in the system.

A. The IT Manager or System Administrator will work with vendors to ensure that proper mechanisms are in place to prevent, detect, contain and correct any security breaches.
B. These mechanisms will include regular system virus checks, security testing and maintenance review of hardware and software for security breaches as prescribed by the vendor.
C. All mechanisms used to manage the security configuration of the system will be documented by the vendor or the Security Officer at regular intervals.
D. Any breaches of security detected by the System Administrator or Manager (IT) will be solved by the Security Officer or discussed with the vendor. Partners of the practice will be informed about security breaches and allowed to comment on solutions designed to respond to them.
E. Security processes will be periodically reviewed and updated by the Security Officer or System Administrator along with the vendor. The Security Officer will conduct an annual risk analysis and devise a plan to manage risk.
F. Any AHL user suspected of intentional involvement in security breaches will be terminated.
G. Any AHL user that is inadvertently involved in a security breach will be offered training and education on system procedures.
H. The IT Manger and/or the System Administrator will periodically conduct training sessions for AHL users to alert them to specific security risks.

Policy: **IT-500.4**: AHL will only integrate connectivity services and equipment that meet or exceed industry- established standards for security.

Policy: **IT-500.5**: AHL will use approved security systems and measures recommended to it by its patient accounting system and other software vendors to protect the integrity, confidentiality and availability of electronic data. AHL will document its selection of security measures and update its documentation periodically.

A. AHL will inventory all software programs and systems that could contain protected health information.
B. Vendors for those software programs will be contacted and asked to provide a diagram and documentation of the security measures and access levels available in the software.
C. The IT Manager for the practice will select an appropriate level of security that includes a minimum of the following: individual authentication of users, access controls, audit trails, physical security, disaster recovery, protection of remote access points, protection of external electronic communications and periodic system assessment recommendations.
D. Documentation of the selection process and the choice of security system will be kept by the IT Manager. Documentation of system security levels will be made available to individuals responsible for implementation.
E. The documentation of the security system and security measures will be updated every three years to ensure that a HIPAA approved level of security is maintained.

Policy: **IT-500.6**: The AHL IT department will internally conduct security audits on services, connectivity and systems on a quarterly basis or when any services, connectivity, or systems have been added or modified. Measures will be taken to make improvements in the security system should they be deemed necessary by AHL.

- The following systems will be audited:
  - Terminal Servers
  - Application Servers
  - Data Servers
  - All Connectivity Devices
  - User Accounts
  - Email Accounts
  - Service Accounts
  - Administrator Accounts
  - Firewall Policies
  - VPN Accounts
  - Virus Protection

Policy: **IT-500.7**: The AHL IT department through external consulting firms will conduct security audits on services, connectivity, and systems on a three-year basis. Measures will be taken to make improvements in the security system should they be deemed necessary by AHL.

The securing of data, for use in this manual, is defined as any method or methodology of securing stored data in a way that prevents unauthorized access and guarantees its uncorrupted availability in the future.

The risk of data security is who or what has access to that data.

To overcome that risk, AHL uses a combination of NOS object security, auditing, redundancy, and user account, password based access security, and physical security. AHL also secures its data through maintaining daily backups and having at least a one-week-old copy off site at all times in a fireproof locked safe. These off site backups are protected and encrypted with a password.

AHL audits and secures data on per user and per user group basis. The following is an example: Mary and John are users on AHL and IT has created a data directory called "Finance" on a server called "AHL data". Mary is part of a user group called "Finance", while John is only part of a user group called "Patient Accounting". IT has given the Finance and Administrative groups access to Finance. In this example, Mary, not John has access to the data directory "Finance". If John were to try to access Finance (even though he does not have access to it) an audit entry would be created and recorded in the AHL security database. Each time John tries to access a directory, he does not have access to, the date, time, machine that he is logged on to and the directory he is trying to access will be recorded (logged). AHL also audits the act of copying, moving, deleting, writing and opening certain files. The following file types are fully audited: protected health information, personnel data and salary information, financial data, financial bank access, financial general ledger and financial accounts payable.

Policy: **IT-500.8**: AHL will back up its essential organizational data using industry standard backup media and equipment that allows restoration in the event of a hardware or software failure. Essential organizational data, for the use of these policies, is defined as any data that could be deemed critical to operations or that would take significant time recreating if lost or corrupted.

Policy: **IT-500.9**: AHL will store offsite copies of the media Policy IT-500.8 on a weekly basis.

- Copies will be maintained in a safety deposit box.

The storing of data, for the use of this manual, is defined as any method or methodology of storing information or knowledge for immediate or future use in a way that guarantees that data's accessibility immediately or in the future.

The risk of data storage is how and where that data is stored.

To overcome that risk AHL uses a mixture of redundancy and Redundant Array of Inexpensive Disks - Five (RAID-5) storage. Depending on the particular situation, the data will either be redundant or stored within a RAID-5 Array. The other two alternatives are that the data can be very easily recreated such that it has no need to have any particular secured storing methodology, or that the system housing the data has no way of providing Redundancy or RAID-5 storage.

Policy: **IT-500.10**: AHL will ensure data is stored in a secure place using redundancy, RAID-5 storage, or some other industry acceptable mean of securely storing data that gives the same effect.

Data presentation, for use in this manual, is defined as any method or methodology of displaying or transmitting AHL data.

The risk of data presentation is how AHL data is transmitted and displayed.

To overcome that risk, AHL uses encryption technologies when appropriate during

transmission through areas that are not contained or controlled by AHL. Examples of such situations requiring encryption are when a AHL user uses VPN technologies or connects to a AHL Terminal Server from a dial-up or VPN connection.

Policy: **IT-500.11**: AHL will not implement wireless networking, unless encrypted or deemed secure by computer industry standards.

Policy: **IT-500.12**: AHL will use encryption technologies when transmitting AHL data through areas not contained or controlled by AHL.

A. AHL will instigate integrity controls and message authentication. Internal networking can be considered secure as long as a user based security system where all users have a specific identification and access code is used.
B. If AHL uses the Internet to transmit data, some form of encryption device will have to be employed.
C. Value added networks, private wires and dial up connections are not subject to the encryption requirement.
D. If the vendor's software offers integrity controls and message authentication AHL will take advantage of those.

Policy: **IT-500.13**: Access to AHL information will be restricted to those AHL users who have a business need to use it.

A. The Information Technology Department will have emergency access to the system. All other types of access to the system will be restricted based on the contextual use of the information (e.g.: insurance department will have access to all data necessary to process and mail out claims); the role of the user (e.g.: therapists will have access to chart notes and medical records but not necessarily insurance information) and/or the type of user (e.g.: some users will be able to view and change data in certain areas of the system while others will only be able to view it or may not be able to see it at all).
B. All AHL users must be given clearance by the IT Manager prior to accessing the system. In order to gain security clearance, the AHL user must have an active position that requires system access. Persons that do not require system access (maintenance, janitors, etc.) will not be given passwords or access to the system.
C. Once access is defined, the Manager (IT) or designee will assign all AHL users individually identifiable passwords. All AHL users will be required to log in to the system using their unique password and the system will log AHL users off after a specified period of time in which there has been no input from the user.
D. The IT Manager or System Administrator will be responsible for maintaining and managing levels of access and user passwords. Our Net users will be required to maintain the confidentiality of their passwords.
E. The System Administrator or IT Manager will run reports to audit system access on a monthly to quarterly basis. Other mechanisms may be put in place to monitor system access from entry points other than user entry.

F. Security incidents will be noted and logged. The System Administrator or IT Manager and vendors or security specialists will address any security breaches.
G. Routine changes to system hardware and software will be validated against the security system to avoid creating inadvertent security weaknesses.

Policy: **IT-500.14**: The IT Department will test all security and backup systems quarterly to ensure that they are operating properly.

SECTION 600 System Emergency Response: Contingency Plans

AHL's risks for System Emergencies are Virus Outbreak, System and Network Intrusions, Site to Site Circuit Loss, Data Loss, Fire, and Power Loss.

Policy: **IT-600.1**: AHL will develop and follow a contingency plan for backup and storage of data to allow for recovery of information/data in the event that the system or network is compromised.

A. The IT department, with input from senior management, will prioritize all software applications and services based on its criticality of data. This will allow priority to be identified when implementing contingencies during System Emergencies.
B. In the event of a Virus Outbreak:
    1. Cut off access to the infected portion or portions of the network up to and including disconnection from the internet and/or internal sites.
    2. Cut off access to the infected system or systems
    3. Notify Senior Management and Managers
    4. Identify who initiated the virus outbreak, if possible
    5. Identify how, where and when the virus outbreak took place
    6. Run virus protection systems
    7. Implement Safeguards to prevent future infections
    8. Delete all suspect data and restore from backup
    9. Reimaged the infection workstation
    10. Update Senior Management and Managers of the status
C. In the event of a System or Network Intrusion:
    1. Cut off access to the affected portion or portions of the network up to and including disconnection from the internet and/or internal sites.
    2. Cut off access to the affected system or systems
    3. Notify Senior Management and Managers
    4. Identify who initiated the intrusion, if possible
    5. Identify how, where and when the intrusion took place
    6. Implement Safeguards to prevent future intrusions
    7. Delete all suspect data and restore from backup
    8. Test the system

D. In the event of Site to Site Circuit Loss:
    1. Diagnose the Circuit
    2. Identify Issue
    3. Notify Senior Management and Managers
        - If Internal Issue, solve problem
        - If Circuit Provider issue, contact Circuit Provider to open incident
    4. Once service is restored, Test the system
    5. Notify Senior Management and Managers of the status
    6. Input incident into Helpdesk
    7. Continue to run tests on circuit for 24-48 hours

E. In the event of Data Loss:
    1. Identify what data was lost
    2. Notify Senior Management and Managers
    3. Identify what caused data loss
    4. Solve issue or replace failing component
    5. Test the system
    6. Restore Data if required
    7. Bring online, the system that experienced loss of data
    8. Update Senior Management and Managers of the status
    9. Input Incident into Helpdesk

F. In the event of Fire Loss:
    1. Locate data Backups
    2. Notify Senior Management and Managers
    3. Find and test replacements for integral equipment that was lost
    4. Test Backups
    5. Restore Data
    6. Input Incident into Helpdesk
    7. Test the system

Policy: **IT-600.2**: AHL will implement power backup for all systems that are integral to the processing of Access Health Louisiana Information.

A. In the event of Power Loss:
    1. Shutdown Systems affected by power loss
    2. Shutdown Battery Backup serving systems affected by power loss
    3. Notify Senior Management and Managers
    4. Identify reason for power loss
        - If Internal issue, solve problem or contact facility management
        - If External issue, contact the Power Company
    5. Once power is restored, Test the system
    6. Update Senior Management and Managers of the status
    7. Wait 10-15 minutes
    8. Restore Battery Backup serving systems affected by power loss
    9. Restore Systems affected by power loss
    10. Input Incident into Helpdesk