EDGEWATER I.T.

INFORMATION SECURITY POLICY

Last Revision Date

10/24/2018 v.3.1

Document Owner

Anthony Bakker - CEO, CIO, CPO, CST, ISO

Table of Contents

Updates to Document

Date	User	Section	Content	Version
11/13/2015	ARB	All	Document Creation	v1.0
11/13/2016	ARB	All	Policy Modification	v2.0
10/24/2017	ARB	All	Policy Modification	V3.0

Edgewater IT, LLC	**Policy and Procedure**
Title: INTRODUCTION	
Approval Date: 11/13/2016	**Review: Annual**
Effective Date: 11/13/2016	**Information Technology**

Introduction

Purpose

This policy defines the technical controls and security configurations users and Information Technology (IT) administrators are required to implement in order to ensure the integrity and availability of the data environment at Edgewater IT, LLC, hereinafter, referred to as **Edgewater IT, LLC**. It serves as a central policy document with which all employees and contractors must be familiar, and defines actions and prohibitions that all users must follow. The policy provides IT managers within Edgewater IT, LLC with policies and guidelines concerning the acceptable use of Edgewater IT, LLC technology equipment, e-mail, Internet connections, voice-mail, facsimile, future technology resources and information processing.

The policy requirements and restrictions defined in this document shall apply to network infrastructures, databases, external media, encryption, hardcopy reports, films, slides, models, wireless, telecommunication, conversations, and any other methods used to convey knowledge and ideas across all hardware, software, and data transmission mechanisms. This policy must be adhered to by all Edgewater IT, LLC employees or temporary workers at all locations and by contractors working with Edgewater IT, LLC as subcontractors.

Scope

This policy document defines common security requirements for all Edgewater IT, LLC personnel and systems that create, maintain, store, access, process or transmit information. This policy also applies to information resources owned by others, such as contractors of Edgewater IT, LLC, entities in the private sector, in cases where Edgewater IT, LLC has a legal, contractual or fiduciary duty to protect said resources while in Edgewater IT, LLC custody. In the event of a conflict, the more restrictive measures apply. This policy covers Edgewater IT, LLC network system, which is comprised of various hardware, software, communication equipment and other devices designed to assist Edgewater IT, LLC in the creation, receipt, storage, processing, and transmission of information. This definition includes equipment connected to any Edgewater IT, LLC domain or VLAN, either hardwired or wirelessly, and includes all stand-alone equipment that is deployed by Edgewater IT, LLC at its office locations or at remote locales.

Acronyms / Definitions

Common terms and acronyms that may be used throughout this document.

CEO – The Chief Executive Officer is responsible for the overall privacy and security Edgewater IT, LLCs of the company.

CIO – The Chief Information Officer

CPO – The Chief Privacy Officer is responsible for HIPAA privacy compliance issues.

CST – Confidentiality and Security Team

ISO – Information Security Officer

DoD – Department of Defense

Encryption – The process of transforming information, using an algorithm, to make it unreadable to anyone other than those who have a specific 'need to know.'

External Media –i.e. CD-ROMs, DVDs, floppy disks, flash drives, USB keys, thumb drives, tapes

FAT – File Allocation Table - The FAT file system is relatively uncomplicated and an ideal format for floppy disks and solid-state memory cards. The most common implementations have a serious drawback in that when files are deleted and new files written to the media, their fragments tend to become scattered over the entire media, making reading and writing a slow process.

Firewall – a dedicated piece of hardware or software running on a computer which allows or denies traffic passing through it, based on a set of rules.

FTP – File Transfer Protocol

HIPAA - Health Insurance Portability and Accountability Act

IT - Information Technology

LAN – Local Area Network – a computer network that covers a small geographic area, i.e. a group of buildings, an office.

NTFS – New Technology File Systems **–** NTFS has improved support for metadata and the use of advanced data structures to improve performance, reliability, and disk space utilization plus additional extensions such as security access control lists and file system journaling. The exact specification is a trade secret of Microsoft.

SOW - Statement of Work - An agreement between two or more parties that details the working relationship between the parties and lists a body of work to be completed.

User - Any person authorized to access an information resource.

Privileged Users – system administrators and others specifically identified and authorized by Edgewater IT, LLC management.

Users with edit/update capabilities – individuals, who are permitted, based on job assignment, to add, delete, or change records in a database**.**

Users with inquiry (read only) capabilities – individuals who are prevented, based on job assignment, from adding, deleting, or changing records in a database. Their system access is limited to reading information only.

VLAN – Virtual Local Area Network – A logical network, typically created within a network device, usually used to segment network traffic for administrative, performance and/or security purposes.
VPN – Virtual Private Network – Provides a secure passage through the public Internet.
WAN – Wide Area Network – A computer network that enables communication across a broad area, i.e. regional, national.
Virus - a software program capable of reproducing itself and usually capable of causing great harm to files or other programs on the computer it attacks. A true virus cannot spread to another computer without human assistance.

Applicable Statutes / Regulations

The following is a list of the various agencies/organizations whose laws, mandates, and regulations were incorporated into the various policy statements included in this document.

N/A

Each of the policies defined in this document is applicable to the task being performed – not just to specific departments or job titles.

Privacy Officer

Edgewater IT, LLC has established a Privacy Officer as required by HIPAA. This Privacy Officer will oversee all ongoing activities related to the development, implementation, and maintenance of Edgewater IT, LLC privacy policies in accordance with applicable federal and state laws. The current Privacy Officer for Edgewater IT, LLC is:

Anthony Bakker 305-814-4446

Confidentiality / Security Team (CST)

Edgewater IT, LLC has established a Confidentiality / Security Team made up of key personnel whose responsibility it is to identify areas of concern within Edgewater IT, LLC and act as the first line of defense in enhancing the appropriate security posture.

All members identified within this policy are assigned to their positions by the CEO. The term of each member assigned is at the discretion of the CEO, but generally, it is expected that the term will be one year. Members for each year will be assigned at the first meeting of the Quality Council in a new calendar year. This committee will consist of the positions within Edgewater IT, LLC most responsible for the overall security policy planning of the organization- the CEO, PO, CMO, ISO, and the CIO (where applicable). The current members of the CST are:

Owner Anthony Bakker 305-814-4446

The CST will meet quarterly to discuss security issues and to review concerns that arose during the quarter. The CST will identify areas that should be addressed during annual training and review/update security policies as necessary.

The CST will address security issues as they arise and recommend and approve immediate security actions to be undertaken. It is the responsibility of the CST to identify areas of concern within Edgewater IT, LLC and act as the first line of defense in enhancing the security posture of Edgewater IT, LLC.

The CST is responsible for maintaining a log of security concerns or confidentiality issues. This log must be maintained on a routine basis, and must include the dates of an event, the actions taken to address the event, and recommendations for personnel actions, if appropriate. This log will be reviewed during the quarterly meetings.

The Privacy Officer (PO) or other assigned personnel is responsible for maintaining a log of security enhancements and features that have been implemented to further protect all sensitive information and assets held by Edgewater IT, LLC. This log will also be reviewed during the quarterly meetings.

Edgewater IT, LLC **Policy and Procedure**	
Title: EMPLOYEE RESPONSIBILITIES	
Approval Date: 11/13/2016	**Review: Annual**
Effective Date: 11/13/2016	**Information Technology**

Employee Responsibilities

Employee Requirements

The first line of defense in data security is the individual Edgewater IT, LLC user. Edgewater IT, LLC users are responsible for the security of all data which may come to them in whatever format. Edgewater IT, LLC is responsible for maintaining ongoing training programs to inform all users of these requirements.

Secure Laptop with a Cable Lock - When out of the office all laptop computers must be secured with the use of a cable lock. Cable locks are provided with all new laptops computers during the original set up. All users will be instructed on their use and a simple user document, reviewed during employee orientation, is included on all laptop computers.

Most Edgewater IT, LLC computers will contain sensitive data either of a medical, personnel, or financial nature, and the utmost care should be taken to ensure that this data is not compromised. Laptop computers are unfortunately easy to steal, particularly during the stressful period while traveling. The cable locks are not fool proof, but do provide an additional level of security. Many laptop computers are stolen in snatch and run robberies, where the thief runs through an office or hotel room and grabs all of the equipment he/she can quickly remove. The use of a cable lock helps to thwart this type of event.

Unattended Computers - Unattended computers should be locked by the user when leaving the work area. This feature is discussed with all employees during yearly security training. Edgewater IT, LLC policy states that all computers will have the automatic screen lock function set to automatically activate upon fifteen (15) minutes of inactivity. Employees are not allowed to take any action which would override this setting.

Home Use of Edgewater IT, LLC Corporate Assets - Only computer hardware and software owned by and installed by Edgewater IT, LLC is permitted to be connected to or installed on Edgewater IT, LLC equipment. Only software that has been approved for corporate use by Edgewater IT, LLC may be installed on Edgewater IT, LLC equipment. Personal computers supplied by Edgewater IT, LLC are to be used solely for business purposes. All employees must read and understand the list of prohibited activities that are outlined below. Modifications or configuration changes are not permitted on computers supplied by Edgewater IT, LLC for home use.

Retention of Ownership - All software programs and documentation generated or provided by employees, consultants, or contractors for the benefit of Edgewater IT, LLC are the property of Edgewater IT, LLC unless covered by a contractual

agreement. Nothing contained herein applies to software purchased by Edgewater IT, LLC employees at their own expense.

Prohibited Activities

Personnel are prohibited from the following activities. The list is not inclusive. Other prohibited activities are referenced elsewhere in this document.

- Crashing an information system. Deliberately crashing an information system is strictly prohibited. Users may not realize that they caused a system crash, but if it is shown that the crash occurred as a result of user action, a repetition of the action by that user may be viewed as a deliberate act.
- Attempting to break into an information resource or to bypass a security feature. This includes running password-cracking programs or sniffer programs, and attempting to circumvent file or other resource permissions.
- Introducing, or attempting to introduce, computer viruses, Trojan horses, peer-to-peer ("P2P") or other malicious code into an information system.

  Exception: Authorized information system support personnel, or others authorized by Edgewater IT, LLC Privacy Officer, may test the resiliency of a system. Such personnel may test for susceptibility to hardware or software failure, security against hacker attacks, and system infection.
- Browsing. The willful, unauthorized access or inspection of confidential or sensitive information to which you have not been approved on a "need to know" basis is prohibited.
- Personal or Unauthorized Software. Use of personal software is prohibited. All software installed on Edgewater IT, LLC computers must be approved by Edgewater IT, LLC.
- Software Use. Violating or attempting to violate the terms of use or license agreement of any software product used by Edgewater IT, LLC is strictly prohibited.
- System Use. Engaging in any activity for any purpose that is illegal or contrary to the policies, procedures or business interests of Edgewater IT, LLC is strictly prohibited.

Electronic Communication, E-mail, Internet Usage

As a productivity enhancement tool, Edgewater IT, LLC encourages the business use of electronic communications. However, all electronic communication systems and all messages generated on or handled by Edgewater IT, LLC owned equipment are considered the property of Edgewater IT, LLC – not the property of individual users. Consequently, this policy applies to all Edgewater IT, LLC employees and contractors, and covers all electronic communications including, but not limited to, telephones, e-mail, voice mail, instant messaging, Internet, fax, personal computers, and servers.

Edgewater IT, LLC provided resources, such as individual computer workstations or laptops, computer systems, networks, e-mail, and Internet software and services are intended for business purposes. However, incidental personal use is permissible if:

1) it does not consume more than a trivial amount of employee time or resources,
2) it does not interfere with staff productivity,
3) it does not preempt any business activity,
4) it does not violate any of the following:

    a) Copyright violations – This includes the act of pirating software, music, books and/or videos or the use of pirated software, music, books and/or videos and the illegal duplication and/or distribution of information and other intellectual property that is under copyright.
    b) Illegal activities – Use of Edgewater IT, LLC information resources for or in support of illegal purposes as defined by federal, state or local law is strictly prohibited.
    c) Commercial use – Use of Edgewater IT, LLC information resources for personal or commercial profit is strictly prohibited.
    d) Political Activities – All political activities are strictly prohibited on Edgewater IT, LLC premises. Edgewater IT, LLC encourages all of its employees to vote and to participate in the election process, but these activities must not be performed using Edgewater IT, LLC assets or resources.
    e) Harassment – Edgewater IT, LLC strives to maintain a workplace free of harassment and that is sensitive to the diversity of its employees. Therefore, Edgewater IT, LLC prohibits the use of computers, e-mail, voice mail, instant messaging, texting and the Internet in ways that are disruptive, offensive to others, or harmful to morale. For example, the display or transmission of sexually explicit images, messages, and cartoons is strictly prohibited. Other examples of misuse include, but is not limited to, ethnic slurs, racial comments, off-color jokes, or anything that may be construed as harassing, discriminatory, derogatory, defamatory, threatening or showing disrespect for others.
    f) Junk E-mail - All communications using IT resources shall be purposeful and appropriate. Distributing "junk" mail, such as chain letters, advertisements, or unauthorized solicitations is prohibited. A chain letter is defined as a letter sent to several persons with a request that each send copies of the letter to an equal number of persons. Advertisements offer services from someone else to you. Solicitations are when someone asks you for something. If you receive any of the above, delete the e-mail message immediately. Do not forward the e-mail message to anyone.

Generally, while it is **NOT** the policy of Edgewater IT, LLC to monitor the content of any electronic communication, Edgewater IT, LLC is responsible for servicing and protecting Edgewater IT, LLC's equipment, networks, data, and resource availability and therefore may be required to access and/or monitor electronic communications from time to time. Several different methods are employed to accomplish these goals. For example, an audit or cost analysis may require reports that monitor phone numbers dialed, length of calls, number of calls to / from a specific handset, the time of day, etc. Other examples where electronic

communications may be monitored include, but are not limited to, research and testing to optimize IT resources, troubleshooting technical problems and detecting patterns of abuse or illegal activity.

Edgewater IT, LLC reserves the right, at its discretion, to review any employee's files or electronic communications to the extent necessary to ensure all electronic media and services are used in compliance with all applicable laws and regulations as well as Edgewater IT, LLC policies.

Employees should structure all electronic communication with recognition of the fact that the content could be monitored, and that any electronic communication could be forwarded, intercepted, printed or stored by others.

Internet Access

Internet access is provided for Edgewater IT, LLC users and is considered a great resource for the organization. This resource is costly to operate and maintain, and must be allocated primarily to those with business, administrative or contract needs. The Internet access provided by Edgewater IT, LLC should not be used for entertainment, listening to music, viewing the sports highlight of the day, games, movies, etc. Do not use the Internet as a radio or to constantly monitor the weather or stock market results. While seemingly trivial to a single user, the company wide use of these non-business sites consumes a huge amount of Internet bandwidth, which is therefore not available to responsible users.

Users must understand that individual Internet usage is monitored, and if an employee is found to be spending an excessive amount of time or consuming large amounts of bandwidth for personal use, disciplinary action will be taken.

Many Internet sites, such as games, peer-to-peer file sharing applications, chat rooms, and on-line music sharing applications, have already been blocked by Edgewater IT, LLC routers and firewalls. This list is constantly monitored and updated as necessary. Any employee visiting pornographic sites will be disciplined and may be terminated.

Reporting Software Malfunctions

Users should inform the appropriate Edgewater IT, LLC personnel when the user's software does not appear to be functioning correctly. The malfunction - whether accidental or deliberate - may pose an information security risk. If the user, or the user's manager or supervisor, suspects a computer virus infection, Edgewater IT, LLC computer virus policy should be followed, and these steps should be taken immediately:

- Stop using the computer
- Do not carry out any commands, including commands to <Save> data.
- Do not close any of the computer's windows or programs.
- Do not turn off the computer or peripheral devices.
- If possible, physically disconnect the computer from networks to which it is attached.

- Inform the appropriate personnel or Edgewater IT, LLC as soon as possible. Write down any unusual behavior of the computer (screen messages, unexpected disk access, unusual responses to commands) and the time when they were first noticed.
- Write down any changes in hardware, software, or software use that preceded the malfunction.
- Do not attempt to remove a suspected virus!

The ISO should monitor the resolution of the malfunction or incident, and report to the CST the result of the action with recommendations on action steps to avert future similar occurrences.

Report Security Incidents

It is the responsibility of each Edgewater IT, LLC employee or contractor to report perceived security incidents on a continuous basis to the appropriate supervisor or security person. A User is any person authorized to access an information resource. Users are responsible for the day-to-day, hands-on security of that resource. Users are to formally report all security incidents or violations of the security policy immediately to the Privacy Officer Users should report any perceived security incident to either their immediate supervisor, or to their department head, or to any member of Edgewater IT, LLC CST. Members of the CST are specified above in this document.

Reports of security incidents shall be escalated as quickly as possible. Each member of Edgewater IT, LLC CST must inform the other members as rapidly as possible. Each incident will be analyzed to determine if changes in the existing security structure are necessary. All reported incidents are logged and the remedial action indicated. It is the responsibility of the CST to provide training on any procedural changes that may be required as a result of the investigation of an incident.

Security breaches shall be promptly investigated. If criminal action is suspected, Edgewater IT, LLC Privacy Officer shall contact the appropriate law enforcement and investigative authorities immediately, which may include but is not limited to the police or the FBI.

Transfer of Sensitive/Confidential Information

When confidential or sensitive information from one individual is received by another individual while conducting official business, the receiving individual shall maintain the confidentiality or sensitivity of the information in accordance with the conditions imposed by the providing individual. All employees must recognize the sensitive nature of data maintained by Edgewater IT, LLC and hold all data in the strictest confidence. Any purposeful release of data to which an employee may have access is a violation of Edgewater IT, LLC policy and will result in personnel action, and may result in legal action.

Transferring Software and Files between Home and Work

Personal software shall not be used on Edgewater IT, LLC computers or networks. If a need for specific software exists, submit a request to your supervisor or department head. Users shall not use Edgewater IT, LLC purchased software on home or on non-Edgewater IT, LLC computers or equipment.

Edgewater IT, LLC proprietary data, including but not limited to patient information, IT Systems information, financial information or human resource data, shall not be placed on any computer that is not the property of Edgewater IT, LLC without written consent of the respective supervisor or department head. It is crucial to Edgewater IT, LLC to protect all data and, in order to do that effectively we must control the systems in which it is contained. In the event that a supervisor or department head receives a request to transfer Edgewater IT, LLC data to a non-Edgewater IT, LLC Computer System, the supervisor or department head should notify the Privacy Officer or appropriate personnel of the intentions and the need for such a transfer of data.

Edgewater IT, LLC Wide Area Network ("WAN") is maintained with a wide range of security protections in place, which include features such as virus protection, e-mail file type restrictions, firewalls, anti-hacking hardware and software, etc. Since Edgewater IT, LLC does not control non-Edgewater IT, LLC personal computers, Edgewater IT, LLC cannot be sure of the methods that may or may not be in place to protect Edgewater IT, LLC sensitive information, hence the need for this restriction.

Internet Considerations

Special precautions are required to block Internet (public) access to Edgewater IT, LLC information resources not intended for public access, and to protect confidential Edgewater IT, LLC information when it is to be transmitted over the Internet.

The following security and administration issues shall govern Internet usage.

Prior approval of Edgewater IT, LLC Privacy Officer or appropriate personnel authorized by Edgewater IT, LLC shall be obtained before:

- An Internet, or other external network connection, is established.
- Edgewater IT, LLC information (including notices, memoranda, documentation and software) is made available on any Internet-accessible computer (e.g. web or ftp server) or device.
- Users may not install or download any software (applications, screen savers, etc.). If users have a need for additional software, the user is to contact their supervisor.
- Use shall be consistent with the goals of Edgewater IT, LLC. The network can be used to market services related to Edgewater IT, LLC, however use of the network for personal profit or gain is prohibited.
- Confidential or sensitive data - including credit card numbers, telephone calling card numbers, logon passwords, and other parameters that can be used to access goods or services - shall be encrypted before being transmitted through the Internet.

- The encryption software used, and the specific encryption keys (e.g. passwords, pass phrases), shall be escrowed with Edgewater IT, LLC Privacy Officer or appropriate personnel, to ensure they are safely maintained/stored. The use of encryption software and keys, which have not been escrowed as prescribed above, is prohibited, and may make the user subject to disciplinary action.

Installation of authentication and encryption certificates on the e-mail system
Any user desiring to transfer secure e-mail with a specific identified external user may request to exchange public keys with the external user. Once verified, the certificate is installed on both recipients' workstations, and the two may safely exchange secure e-mail.

Use of WinZip encrypted and zipped e-mail
This software allows Edgewater IT, LLC personnel to exchange e-mail with remote users who have the appropriate encryption software on their system. The two users exchange private keys that will be used to both encrypt and decrypt each transmission. Any Edgewater IT, LLC staff member who desires to utilize this technology may request this software from the Privacy Officer or appropriate personnel.

Edgewater IT, LLC **Policy and Procedure**	
Title: IDENTIFICATION and AUTHENTICATION	
Approval Date: 11/13/2016	**Review: Annual**
Effective Date: 11/13/2016	**Information Technology**

Identification and Authentication

User Logon IDs

Individual users shall have unique logon ids and passwords. An access control system shall identify each user and prevent unauthorized users from entering / using information resources. Security requirements for user identification include:

- Each user shall be assigned a unique identifier.
- Users shall be responsible for the use/misuse of their individual logon id.

All user login ids are audited at least twice yearly and all inactive logon ids are revoked.

The logon id is locked/revoked after a maximum of three (3) unsuccessful logon attempts which then require the passwords to be reset by the appropriate Administrator.

Passwords

User Account Passwords

User ids and passwords are required in order to gain access to all Edgewater IT, LLC networks and workstations. All passwords are restricted by a corporate wide password policy to be of a "complex" nature. This means that all passwords must conform to restrictions and limitations that are designed to make the password difficult to guess. Users are required to select a password in order to obtain access to any electronic information both at the server level and at the workstation level. When passwords are reset, the user will be automatically prompted to manually change that assigned password.

Password Length – Passwords are required to be a minimum of eight characters[15].

Content Requirements - Passwords must contain a combination of upper and lower case alphabetic characters, numeric characters, and special characters.

Change Frequency – Passwords must be changed every 90 days. Compromised passwords shall be changed immediately.
Reuse - The previous twenty for (24) passwords cannot be reused.
Restrictions on Sharing Passwords - Passwords shall not be shared, or written down on paper, or stored within a file or database on a workstation, and must be kept confidential.
Restrictions on Recording Passwords - Passwords are masked or suppressed on all online screens, and are never printed or included in reports or logs. Passwords are stored in an encrypted format.

Access Control

Information resources are protected using access control systems. Access control systems include both internal (passwords, encryption, access control lists, constrained user interfaces) and external (port protection devices, firewalls, host-based authentication).

Rules for access to resources (including internal and external telecommunications and networks) have been established by the information/application owner or manager responsible for the resources. Access is granted only by Edgewater IT, LLC. This form can only be initiated by the appropriate department head, and must be signed by the department head, and by the Privacy Officer or appropriate personnel.

Computer banner screens, if used, shall contain statements to the effect that unauthorized use of the system is prohibited, and that violators will be subject to criminal prosecution.

Identification and Authentication Requirements

The host security management program shall maintain current user application activity authorizations. Each initial request for a connection or a session is subject to the authorization process previously addressed.

Edgewater IT, LLC **Policy and Procedure**	
Title: NETWORK CONNECTIVITY	
Approval Date: 11/13/2016	**Review: Annual**
Effective Date: 11/13/2016	**Information Technology**

Network Connectivity

Remote/Dial in Connections

Access to Edgewater IT, LLC information resources through high speed internet, modems or other dial-in devices / software, if available, shall be subject to authorization and authentication by an access control system. **Direct inward dialing without passing through the access control system is prohibited.**

Permanent Connections

The security of Edgewater IT, LLC systems can be jeopardized from third party locations if security Edgewater IT, LLCs and resources are inadequate. When there is a need to connect to a third-party location, a risk analysis should be conducted. The risk analysis should consider the type of access required the value of the information, the security measures employed by the third party, and the implications for the security of Edgewater IT, LLC systems. The Privacy Officer or appropriate personnel should be involved in the process, design and approval.

Emphasis on Security in Third Party Contracts

Access to Edgewater IT, LLC computer systems or corporate networks should not be granted until a review of the following concerns have been made, and appropriate restrictions or covenants included in a statement of work ("SOW") with the party requesting access.

- Applicable sections of Edgewater IT, LLC Information Security Policy have been reviewed and considered.
- Policies and standards established in Edgewater IT, LLC information security program
  have been enforced.
- A risk assessment of the additional liabilities that will attach to each of the parties to the agreement.
- The right to audit contractual responsibilities should be included in the agreement or SOW.
- Arrangements for reporting and investigating security incidents must be included in the agreement in order to meet the covenants of the HIPAA Business Associate Agreement.
- A description of each service to be made available.
- Each service, access, account, and/or permission made available should only be the minimum necessary for the third party to perform their contractual obligations.

- A detailed list of users that have access to Edgewater IT, LLC computer systems must be maintained and auditable.
- If required under the contract, permission should be sought to screen authorized users.
- Dates and times when the service is to be available should be agreed upon in advance.
- Procedures regarding protection of information resources should be agreed upon in advance and a method of audit and enforcement implemented and approved by both parties.
- The right to monitor and revoke user activity should be included in each agreement.
- Language on restrictions on copying and disclosing information should be included in all agreements.
- Responsibilities regarding hardware and software installation and maintenance should be understood and agreement upon in advance.
- Measures to ensure the return or destruction of programs and information at the end of the contract should be written into the agreement.
- If physical protection measures are necessary because of contract stipulations, these should be included in the agreement.
- A formal method to grant and authorized users who will access to the data collected under the agreement should be formally established before any users are granted access.
- Mechanisms should be in place to ensure that security measures are being followed by all parties to the agreement.
- Because annual confidentiality training is required under the HIPAA regulation, a formal procedure should be established to ensure that the training takes place, that there is a method to determine who must take the training, who will administer the training, and the process to determine the content of the training established.
- A detailed list of the security measures which will be undertaken by all parties to the agreement should be published in advance of the agreement.

Firewalls

Authority from the Privacy Officer or appropriate personnel must be received before any employee or contractor is granted access to an Edgewater IT, LLC router or firewall.

Edgewater IT, LLC **Policy and Procedure**	
Title: MALICIOUS CODE	
Approval Date: 11/13/2016	**Review: Annual**
Effective Date: 11/13/2016	**Information Technology**

Malicious Code:

Antivirus Software Installation

Antivirus software is installed on all Edgewater IT, LLC personal computers and servers. Virus update patterns are updated daily on Edgewater IT, LLC servers and workstations. Virus update engines and data files are monitored by appropriate administrative staff that is responsible for keeping all virus patterns up to date.

> Configuration - The antivirus software currently implemented by Edgewater IT, LLC is Windows Defender. Updates are received directly from Microsoft which is scheduled daily.
> Remote Deployment Configuration - Through an automated procedure, updates and virus patches may be pushed out to the individual workstations and servers on an as needed basis.

New Software Distribution

Only software created by Edgewater IT, LLC application staff, if applicable, or software approved by the Privacy Officer or appropriate personnel will be used on internal computers and networks. A list of approved software is maintained in Appendix A. All new software will be tested by appropriate personnel in order to ensure compatibility with currently installed software and network configuration. In addition, appropriate personnel must scan all software for viruses before installation. This includes shrink-wrapped software procured directly from commercial sources as well as shareware and freeware obtained from electronic bulletin boards, the Internet, or on disks (magnetic or CD-ROM and custom-developed software).

Although shareware and freeware can often be useful sources of work-related programs, the use and/or acquisition of such software must be approved by the Privacy Officer or appropriate personnel. Because the software is often provided in an open distribution environment, special precautions must be taken before it is installed on Edgewater IT, LLC computers and networks. These precautions include determining that the software does not, because of faulty design, "misbehave" and interfere with or damage Edgewater IT, LLC hardware, software, or data, and that the software does not contain viruses, either originating with the software designer or acquired in the process of distribution.

All data and program files that have been electronically transmitted to a Edgewater IT, LLC computer or network from another location must be scanned for viruses immediately after being received. Contact the appropriate Edgewater IT, LLC personnel for instructions for scanning files for viruses.

Every diskette, CD-ROM, DVD and USB device is a potential source for a computer virus. Therefore, every diskette, CD-ROM, DVD and USB device must be scanned for virus infection prior to copying information to a Edgewater IT, LLC computer or network.

Computers shall never be "booted" from a diskette, CD-ROM, DVD or USB device received from an outside source. Users shall always remove any diskette, CD-ROM, DVD or USB device from the computer when not in use. This is to ensure that the diskette, CD-ROM, DVD or USB device is not in the computer when the machine is powered on. A diskette, CD-ROM, DVD or USB device infected with a boot virus may infect a computer in that manner, even if the diskette, CDROM, DVD or USB device is not "bootable".

Retention of Ownership

All software programs and documentation generated or provided by employees, consultants, or contractors for the benefit of Edgewater IT, LLC are the property of Edgewater IT, LLC unless covered by a contractual agreement. Employees developing programs or documentation must sign a statement acknowledging Edgewater IT, LLC ownership at the time of employment. Nothing contained herein applies to software purchased by Edgewater IT, LLC employees at their own expense.

Edgewater IT, LLC **Policy and Procedure**	
Title: ENCRYPTION	
Approval Date: 11/13/2016	**Review: Annual**
Effective Date: 11/13/2016	**Information Technology**

Encryption

Definition

The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text*;* encrypted data is referred to as cipher text**.**

Encryption Key

An encryption key specifies the particular transformation of plain text into cipher text, or vice versa during decryption.

If justified by risk analysis, sensitive data and files shall be encrypted before being transmitted through networks. When encrypted data are transferred between agencies, the agencies shall devise a mutually agreeable procedure for secure key management. In the case of conflict, Edgewater IT, LLC shall establish the criteria in conjunction with the Privacy Officer or appropriate personnel. Edgewater IT, LLC employs several methods of secure data transmission and storage.

Outlook Message Encryption in the e-mail system

Any user desiring to transfer confidential information with a specific identified external user will use Outlook Message Encryption. Files may be emailed using Outlook Message Encryption through the use of appropriate security keywords in body and subject line- Private

Use of WinZip encrypted and zipped e-mail

This software allows Edgewater IT, LLC personnel to exchange e-mail with remote users who have the appropriate encryption software on their system. The two users exchange private keys that will be used to both encrypt and decrypt each transmission. Any Edgewater IT, LLC staff member who desires to utilize this technology may request this software from the Privacy Officer or appropriate personnel.

Computer Hard Drive Encryption

All Edgewater IT, LLC computers shall utilize Bit locker hard drive encryption. Recovery keys are located in the Microsoft Cloud.

Confidential Files (Password File)

All client password files are encrypted with a password. Password files are in a VeraCrypt encrypted file volume that must be mounted in order to access the files within. Volume is dismounted when not in use. Encrypted volume is synched to the Microsoft Cloud.

Edgewater IT, LLC **Policy and Procedure**	
Title: BUILDING SECURITY	
Approval Date: 11/13/2016	**Review: Annual**
Effective Date: 11/13/2016	**Information Technology**

Building Security

It is the policy of Edgewater IT, LLC to provide building access in a secure manner. Each site, if applicable, is somewhat unique in terms of building ownership, lease contracts, entranceway access, fire escape requirements, and server room control. However, Edgewater IT, LLC strives to continuously upgrade and expand its security and to enhance protection of its assets and medical information that has been entrusted to it. The following list identifies measures that are in effect at Edgewater IT, LLC. All other facilities, if applicable, have similar security appropriate for that location.

Description of building, location, square footage, and the use of any generator.

- Entrance to the building during non-working hours is controlled by a security fob[21]. Attempted entrance without this fob results in no access.
- Only specific Edgewater IT, LLC employees are given the security code for entrance. Disclosure of the security code to non-employees is strictly prohibited.
- The door to the reception area is locked between the hours of 5:00 PM to 9:00AM M-F and locked Sat-Sun and requires appropriate credentials or escort past the reception or waiting area door(s).
- The reception area is staffed always during the working hours of 9:00 AM to 5:00 PM.
- Any unrecognized person in a restricted office location should be challenged as to their right to be there. All visitors must sign in at the front desk.

- The building is equipped with security cameras to record activities in the parking lot and within the area encompassing the front entrance. All activities in these areas are recorded on a 24 hour a day 365 day per year basis[26].
- Fire Protection: Use of local building codes will be observed. Manufacturer's recommendations on the fire protection of individual hardware will be followed.

Edgewater IT, LLC **Policy and Procedure**	
Title: TELECOMMUTING	
Approval Date: 11/13/2016	**Review: Annual**
Effective Date: 11/13/2016	**Information Technology**

Telecommuting

With the increased availability of broadband access and VPNs, telecommuting has become more viable for many organizations. Edgewater IT, LLC considers telecommuting to be an acceptable work arrangement in certain circumstances. This policy is applicable to all employees who work either permanently or only occasionally outside of Edgewater IT, LLC office environment. It applies to users who work from their home full time, to employees on temporary travel, to users who work from a remote office location, and to any user who connects to Edgewater IT, LLC network from a remote location.

While telecommuting can be an advantage for users and for the organization in general, it presents new risks in the areas of confidentiality and security of data. Workers linked to Edgewater IT, LLC's network become an extension of the wide area network and present additional environments that must be protected against the danger of spreading Trojans, viruses, or other malware. This arrangement also exposes the corporate as well as patient data to risks not present in the traditional work environment.

General Requirements

Telecommuting workers are required to follow all corporate, security, confidentiality, HR, or Code of Conduct policies that are applicable to other employees/contractors.

- **Need to Know:** Telecommuting Users will have the access based on the same 'need to know' as they have when in the office.
- **Password Use:** The use of a strong password, changed at least every 90 days, is even more critical in the telecommuting environment. Do not share your password or write it down where a family member or visitor can see it.
- **Training:** Personnel who telecommute must complete the same annual privacy training as all other employees.
- **Contract Specific:** There may be additional requirements specific to the individual contracts to which an employee is assigned.

Required Equipment

Employees approved for telecommuting must understand that Edgewater IT, LLC will not provide all equipment necessary to ensure proper protection of information to which the employee has access; however, the following lists define the equipment and environment required:

Edgewater IT, LLC Provided:

Laptop or Workstation

Employee Provided:

Broadband connection and fees,

Hardware Security Protections

Virus Protection**:** Home users must never stop the update process for Virus Protection. Virus Protection software is installed on all Edgewater IT, LLC personal computers and is set to update the virus pattern daily. This update is critical to the security of all data, and must be allowed to complete.

VPN and Firewall Use**:** Established procedures must be rigidly followed when accessing Edgewater IT, LLC information of any type. Edgewater IT, LLC requires the use of a VPN or Remote Desktop Connector (utilizing secure RD gateway) and a firewall device. Disabling a virus scanner or firewall is reason for termination.

Security Locks: Use security cable locks for laptops at all times, even if at home or at the office. Cable locks have been demonstrated as effective in thwarting robberies.

Lock Screens**:** No matter what location, always lock the screen before walking away from the workstation.

Data Security Protection

Data Backup**:** Backup procedures have been established that encrypt the data being moved to an external media. Use only that procedure – do not create one on your own. If there is not a backup procedure established or if you have external media that is not encrypted, contact the appropriate Edgewater IT, LLC personnel for assistance. Protect external media by enabling BitLocker and keeping it in your possession when traveling.

Transferring Data to Edgewater IT, LLC**:** Transferring of data to Edgewater IT, LLC requires the use of an approved encrypted VPN connection to ensure the confidentiality and integrity of the data being transmitted. Do not circumvent established procedures, nor create your own method when transferring data to Edgewater IT, LLC.

External System Access: If you require access to an external system, contact your supervisor or department head. Privacy Officer or appropriate personnel will assist in establishing a secure method of access to the external system.

E-mail: Do not send any individual-identifiable information (PHI or PII) via e-mail unless it is encrypted. If you need assistance with this, contact the Privacy Officer or appropriate personnel to ensure an approved encryption mechanism is used for transmission through e-mail.

Non-Edgewater IT, LLC Networks: Extreme care must be taken when connecting Edgewater IT, LLC equipment to a home or hotel network. Although Edgewater IT, LLC actively monitors its security status and maintains organization wide protection policies to protect the data within all contracts, Edgewater IT, LLC has

no ability to monitor or control the security procedures on non-Edgewater IT, LLC networks.

Protect Data in Your Possession: View or access only the information that you have a need to see to complete your work assignment. Regularly review the data you have stored to ensure that the amount of client data is kept at a minimum and that old data is eliminated as soon as possible. Store electronic data only in encrypted drives. If your laptop has not been set up with an drives, contact the Privacy Officer or appropriate personnel for assistance.

Hard Copy Reports or Work Papers: Never leave paper records around your work area. Lock all paper records in a file cabinet at night or when you leave your work area.

Data Entry When in a Public Location: Do not perform work tasks which require the use of sensitive corporate or client level information when you are in a public area, i.e. airports, airplanes, hotel lobbies. Computer screens can easily be viewed from beside or behind you.

Sending Data Outside Edgewater IT, LLC**:** All external transfer of data must be associated with an official contract, non-discloser agreement, or appropriate Business Associate Agreement. Do not give or transfer any patient level information to anyone outside Edgewater IT, LLC without the written approval of your supervisor.

Disposal of Paper and/or External Media

Shredding: All paper which contains sensitive information that is no longer needed must be shredded using cross cut shredders which produce particles that are 1 mm x 5 mm (0.04 in. x 0.2 in.) in size (or smaller) before being disposed. Do not place in a trash container without first shredding. All employees working from home, or other non-Edgewater IT, LLC work environment, MUST have direct access to a shredder.

Disposal of Electronic Media: All external media must be sanitized or destroyed in accordance with **NIST SP 800-88 Rev. 1** compliant procedures.

- Do not throw any media containing sensitive, protected information in the trash.
- Return all external media to your supervisor
- External media must be wiped clean of all data. The Privacy Officer or appropriate personnel have very definitive procedures for doing this – so all external media must be sent to them.
- The final step in this process is to forward the media for disposal by a certified destruction agency.

Edgewater IT, LLC **Policy and Procedure**	
Title: SPECIFIC PROTOCOLS AND DEVICES	
Approval Date: 11/13/2016	**Review: Annual**
Effective Date: 11/13/2016	**Information Technology**

Specific Protocols and Devices

Wireless Usage Standards and Policy

Due to an emergence of wireless access points in hotels, airports, and in homes, it has become imperative that a Wireless Usage policy be developed and adopted to ensure the security and functionality of such connections for Edgewater IT, LLC employees. This policy outlines the processes and procedures for acquiring wireless access privileges, utilizing wireless access, and ensuring the security of Edgewater IT, LLC laptops and mobile devices.

Approval Procedure - In order to be granted the ability to utilize the wireless network interface on your Edgewater IT, LLC laptop or mobile device you will be required to gain the approval of your immediate supervisor or department head and the Privacy Officer or appropriate personnel of Edgewater IT, LLC. The Network Access Request Form (found in Appendix A) is used to make such a request. Once this form is completed and approved you will be contacted by appropriate Edgewater IT, LLC personnel to setup your laptop.

Software Requirements - The following is a list of minimum software requirements for any Edgewater IT, LLC laptop that is granted the privilege to use wireless access:

- Windows 10 Professional or Enterprise (Firewall enabled)
- Antivirus software (Windows Defender)
- Full Disk Encryption (BitLocker)
- Appropriate VPN Client, if applicable

If your laptop does not have all of these software components, please notify your supervisor or department head so these components can be installed.

Use of Transportable Media

Transportable media included within the scope of this policy includes, but is not limited to, SD cards, DVDs, CD-ROMs, and USB key devices.

The purpose of this policy is to guide employees of Edgewater IT, LLC in the proper use of transportable media when a legitimate business requirement exists to transfer data to and from Edgewater IT, LLC networks. Every workstation or server that has been used by either Edgewater IT, LLC employees is presumed to have sensitive information stored on its hard drive. Therefore, procedures must be carefully followed when copying data to or from transportable media to protect sensitive Edgewater IT, LLC data. Since transportable media, by their very design are easily lost, care and protection of these devices must be addressed. Since it is very unlikely that transportable media will be provided to a Edgewater IT, LLC employee by an external source for the exchange of information, it is still necessary that all employees have guidance in the appropriate use of media from other companies.

The use of transportable media in various formats is uncommon with Edgewater IT, LLC within Edgewater IT, LLC. All users must be aware that sensitive data could potentially be lost or compromised when moved outside of Edgewater IT, LLC networks. Transportable media received from an external source could potentially pose a threat to Edgewater IT, LLC networks. ***Sensitive data*** includes all human resource data, financial data, Edgewater IT, LLC proprietary information, and client information.

USB key devices are handy devices which allow the transfer of data in an easy to carry format. They provide a much-improved format for data transfer when compared to previous media formats, like diskettes, CD-ROMs, or DVDs. The software drivers necessary to utilize a USB key are normally included within the device and install automatically when connected. They now come in a rugged titanium format which connects to any key ring. These factors make them easy to use and to carry, but unfortunately easy to lose.

Rules governing the use of transportable media include:

- No ***sensitive data*** should ever be stored on transportable media unless the data is maintained in an encrypted format.
- All USB keys used to store Edgewater IT, LLC data or sensitive data must be a Bitlocker encrypted USB. The use of a personal USB key is strictly prohibited.
- Users must never connect their transportable media to a workstation that is not issued by Edgewater IT, LLC.
- Non-Edgewater IT, LLC workstations and laptops may not have the same security protection standards required by Edgewater IT, LLC, and accordingly virus patterns could potentially be transferred from the non-Edgewater IT, LLC device to the media and then back to Edgewater IT, LLC workstation.

Example: Do not copy a work spreadsheet to your USB key and take it home to work on your home PC.

- Data may be exchanged between Edgewater IT, LLC workstations/networks and workstations used within Edgewater IT, LLC. The very nature of data exchange requires that under certain situations data be exchanged in this manner.

  Examples of necessary data exchange include:
  Data provided to auditors via USB key during the course of the audit.

- It is permissible to connect transferable media from other businesses or individuals into Edgewater IT, LLC workstations or servers as long as the source of the media in on Edgewater IT, LLC Approved Vendor.
- Before initial use and before any ***sensitive data*** may be transferred to transportable media, the media must be sent to the Privacy Officer or appropriate personnel to ensure appropriate and approved encryption is used. Copy ***sensitive data*** only to the encrypted space on the media. Non-sensitive data may be transferred to the non-encrypted space on the media.
- Report all loss of transportable media to your supervisor or department head. It is important that Edgewater IT, LLC Privacy Officer is notified either directly from the employee or contractor or by the supervisor or department head immediately.
- When an employee leaves Edgewater IT, LLC, all transportable media in their possession must be returned to the Privacy Officer or appropriate personnel for data erasure that conforms to US Department of Defense standards for data elimination.

Edgewater IT, LLC utilizes an approved method of encrypted data to ensure that all data is converted to a format that cannot be decrypted. The Privacy Officer or appropriate personnel can quickly establish an encrypted partition on your transportable media.

When no longer in productive use, all Edgewater IT, LLC laptops, workstation, or servers must be wiped of data in a manner which conforms to US Department of Defense standards for data elimination. All transportable media must be wiped according to the same standards. Thus all transportable media must be returned to the Privacy Officer or appropriate personnel for data erasure when no longer in use.

Edgewater IT, LLC **Policy and Procedure**	
Title: DISPOSAL OF EXTERNAL MEDIA / HARDWARE	
Approval Date: 11/13/2016	**Review: Annual**
Effective Date: 11/13/2016	**Information Technology**

Disposal of External Media / Hardware

Disposal of External Media

It must be assumed that any external media in the possession of an employee is likely to contain information. Accordingly, external media (CD-ROMs, DVDs, diskettes, USB drives) should be disposed of in a method that ensures that there will be no loss of data and that the confidentiality and security of that data will not be compromised.

The following steps must be adhered to:

- It is the responsibility of each employee to identify media which should be shredded and to utilize this policy in its destruction.
- External media should never be thrown in the trash.
- When no longer needed all forms of external media are to be sent to the Privacy Officer or appropriate personnel for proper disposal.
- The media will be secured until appropriate destruction methods are used based on NIST 800-88 guidelines.

Requirements Regarding Equipment

All equipment to be disposed of will be wiped of all data, and all settings and configurations will be reset to factory defaults. No other settings, configurations, software installation or options will be made. Asset tags and any other identifying logos or markings will be removed.

Disposition of Excess Equipment

As the older Edgewater IT, LLC computers and equipment are replaced with new systems, the older machines are held in inventory for a wide assortment of uses:

- Older machines are regularly utilized for spare parts.
- Older machines are used on an emergency replacement basis.
- Older machines are used for testing new software.
- Older machines are used as backups for other production equipment.
- Older machines are used when it is necessary to provide a second machine for personnel who travel on a regular basis.
- Older machines are used to provide a second machine for personnel who often work from home.

Appendix A – Approved Software

The following list has been approved for use by Edgewater IT, LLC. All software must be installed and maintained by the appropriate Edgewater IT, LLC personnel.

Software	Version	Approved by	Date	Description/Comments
Office 2016 Professional	16.			
Veracrypt				Used for unlocking encrypted volume
Winzip 20.0				
Eraser	6.2			Secure file erase
MS Project Pro	2013			
Wireshark	2.0.1			Network Analyzer
NMap	7.0.1			
Macrium Reflect				Disk Imaging
HD Tune Pro	5.60			Disk Analyzer
Snagit	8			Image Capture
Virtual Clone Drive				ISO Mount
AD tidy	2.1.7			
Nero Burning Rom				
WinUndelete				
Languard NetScan				
PDF Element				
Hyena				
Magical Jellybean Key Finder				
Azure AD				
ConnectWise				
Remote Utilities				
Google Chrome				
Firefox				
Vlc media Player				
Backrex				

Appendix B – Approved Vendors

Vendor	Primary Contact	Main Number	Product / Service	Description/Comments
NewEgg				
Amazon				
Ebay				
Provantage				