Catholic Health	CATHOLIC HEALTH Rockville Centre, New York IT Security & Privacy Policies and Procedures	Policy Number: 001A Effective Date: 01/21/2013 Last Revision Date: 03/30/2022
	TITLE: 001A – Affiliate Practice Acceptable Use Policy	

PURPOSE:

Catholic Health and System Affiliates (collectively, CH) relies on its information and Information Technology Resources (Resources) to support its business processes. To ensure that its Resources are used properly by its employees, independent contractors, agents, and other Users, CH has implemented this *Affiliate Practice Acceptable Use Policy (AUP).*

POLICY:

1. **Compliance**

   a. This Policy applies to all Users of CH's Resources, wherever the User may be located. It is each User's duty to use CH's Resources responsibly, professionally, ethically, and lawfully. All third-party users (e.g., affiliates, vendors, contractors, regulatory surveyors, volunteers, etc.) will also be required to sign, in order to obtain access to the Environment, the Affiliate Practice Acceptable Use Policy Acknowledgment Form verifying that he or she has read, understands, and agrees to follow this Acceptable Use Policy. Access to the organization's information and systems by external parties is not permitted until due diligence has been conducted and the appropriate controls have been implemented.

   b. Each User is responsible for the security of the Information Technology Environment. A User should immediately notify their CH contact or the CH Service Desk if he or she feels that security may have been compromised in any way.

   c. Any violation of this Policy may lead to disciplinary action which will be based on the severity and context of the violation and shall be in accordance with all existing CH policies and/or appropriate legal action. Disciplinary action may include without limitation, verbal or written reprimand, suspension or termination of agreement and/or appropriate legal action. The CH Chief Information Security Officer (CISO) or his designee may temporarily deny or revoke access privileges if there is a reasonable belief that a violation has occurred. Access privileges may be restored only after consultation between the CISO and CH Management and/or CH Senior Management personnel.

d. The policies stated in this AUP are intended as directives only for CH Resource access and usage. The language should not be construed as creating a contract of employment, express or implied, between CH and any CH system user. In addition, no provision of this AUP shall create an employer-employee relationship between CH and any User who is not a CH employee, such as an affiliate contractor, Affiliate Practice vendor, or other User of CH Resources who is not a CH employee.

e. CH reserves the right to add, delete, or revise any provision of the AUP at any time, or any Information Security Policy without prior notice to Users.

2. No Expectation of Privacy

a. ***No Expectation of Privacy***. The CH Resources and User accounts are issued to Users to assist them in the performance of their jobs, and as such, remain the property of CH. Users do not have an expectation of privacy in anything Users create, store, send, or receive on CH Resources. Resources and access to CH Resources are to be used solely for the purpose of CH business, the User's usual duties, and or other purposes authorized by management.

b. ***Waiver of Privacy Rights***. Users expressly waive any right of privacy in anything Users create, store, send, or receive on CH Resources, through the Internet or any other CH Network. Users consent to allowing authorized CH IT Services personnel to access and review all materials Users create, store, send, or receive on CH Resources. CH may, but is not obligated to, use human or automated means to monitor use of its Resources, at its discretion.

c. ***No Privacy in Communication***. Users must never consider electronic communications to be either private or secure. E-mail could potentially be stored indefinitely on any number of CH Resources as well as non CH resources. Copies of your message may be forwarded to others electronically or on paper. In addition, e-mail sent to nonexistent or incorrect usernames may be delivered to the wrong person(s).

3. Prohibited Activities

a. ***Inappropriate or Unlawful Material***. Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate may not be sent by e-mail, electronic text messages or any other form of electronic communication (such as bulletin board systems, newsgroups, chat groups) or displayed on or stored in any CH Resource. Users encountering or receiving this kind of material should immediately report the incident to the CISO via their CH contact, or the CH Service Desk.

b. ***Prohibited Uses***. CH Resources may not be used for dissemination or storage of commercial or personal advertisements, solicitations, promotions, destructive programs (viruses), political material, or any other use prohibited by this Policy.

c. ***Waste of IT Resources***. Users may not perform acts that waste CH Resources or unfairly monopolize CH Resources to the exclusion of other Users. These acts include, but are not limited to: sending non-business related mass distribution e-mails or chain letters;

subscribing to non-business related mailing lists; spending excessive amounts of time on the Internet; social networking; playing non-business related computer games, music or video; or otherwise creating unnecessary network traffic.

d. ***Communication of Confidential Information***. Unless expressly authorized by CH Senior Management, sending, transmitting, or otherwise disseminating proprietary data, trade secrets or other confidential information, including medical records and/or patient data is strictly prohibited. Always keep in mind that e-mail and the Internet are public methods of communication. When you send information via e-mail or make it available on the Internet, there is always a possibility that the information will be viewed by unauthorized individuals. This type of information is a valuable asset of the company and each of us must make sure that it is protected from unauthorized disclosure.

e. ***Altering Identity (Spoofing)***. Users may not alter the "From:" line or other attribution-of-origin information in e-mail, messages, or postings. Anonymous or pseudonymous electronic communication is forbidden. Users must identify themselves honestly and accurately when sending e-mail.

f. ***Personal Use***. Any use of CH Resources not approved by CH IT Management is prohibited. CH management is aware that personal communications between CH coworkers and external contacts does occur, as well as some limited personal use. Management expects Users to limit such communications and personal use to a minimum. Excessive or abusive volumes of personal communications, activities of a personal nature that tie up resources or employees, or violate any other provision of this agreement are expressly prohibited. Users are reminded that there are no expectations of privacy when using CH Systems.

g. ***Software and Copyright Violations***. The distribution, retrieval, or reproduction of any material without the permission of the copyright holder is expressly prohibited. The import or installation of any software which has not been properly authorized and purchased by CH IT management is expressly prohibited. No User may modify, revise, transform, adapt, disassemble, decompile, or otherwise alter any software licensed to CH without prior written authorization from CH.

h. ***No Forward Policy***. Some information that is transmitted via electronic communications is intended for specific individuals, and therefore, should not be shared with others. Users should exercise caution when forwarding communications to other CH users. CH information that is sensitive in nature may not be forwarded to external parties without the expressed permission of senior management. CH email users are prohibited from modifying the settings of their email account or otherwise causing email received by them to be automatically forwarded to a non CHLI.ORG email address.

4. Logins and Passwords

a. ***Login Accounts***. A unique login account consisting of a User ID and password (see sections 4.b, 4.c, 4.d) is required for each User of the IT Environment. Users are responsible for all transactions made using his or her User ID. No User may access CH

Resources using another User's account. All Users are expected to logoff the workstation when they are away from their work area for extended periods of time. All Users are required to logoff at the end of each day before they leave. Users may not disguise their identity while using any CH Resource.

b. ***Responsibility for Passwords***. Users are responsible for safeguarding their passwords for access to CH Resources. Individual passwords should not be printed, stored online, shared or given to others. Users are prohibited from using or disclosing another User's password.

c. ***Password Maintenance***. Passwords should be obscure and a minimum of eight characters in length. Passwords must include at least one upper case letter, one lower case letter and one number or special character ("@","!","&","%"). All passwords must be changed every 365 days. Users who do not change their password within the time specified will be locked out of the system. .

d. ***Passwords do not Imply Privacy***. Use of passwords to gain access to CH Resources does not imply that Users have an expectation of privacy in the material they create or receive on CH Resources. CH has the right to inspect and or read and or print without prior notice, all material stored on CH Resources.

e. ***Disclosure of Information***. All information accessed by Users of CH systems is to be kept confidential, and only discussed or shared with another User who has been properly authorized to view the information as part of his or her job responsibilities. Information is stored with the expectation that it will only be used or accessed by authorized persons.

5. Security

a. ***Physical Security***. Users shall take all reasonable and prudent measures to physically secure all CH Resources. Users shall not attempt to circumvent any system that secures CH Resources or its components.

b. ***Accessing Other Computers and Networks***. A User's ability to connect to other computers or networks does not imply a right to connect to those systems or to make use of those systems unless specifically authorized by the operators of those systems. Users should not view any information without proper authorization.

c. ***Computer Security***. Each User is responsible for ensuring that the use of external computers and networks, such as the Internet, does not compromise the security of the CH Environment. This duty includes preventing intruders from accessing the CH Network without authorization and taking reasonable precautions to avoid the introduction and spread of viruses, malware and other harmful software. No CH Devices shall leave the continental US without permission from the Office of the CISO.

d. ***Information Technology Security***. Users shall not connect to the CH Network by any means other than by those specifically defined by the CH IT Security Office. Personally owned computers should not be connected to the CH Network without prior approval of

the CH IT Security Office. Users shall not disable CH Resource functions (passwords, virus scan, distribution software, audit trails) implemented by CH IT Services.

e. ***Information Exchange Security.*** CH shall establishes terms and conditions, consistent with any trust relationship established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to (i) access the information system from external information systems; and (ii) process, store or transmit organization-controlled information using external information systems. CH ensures that communications protection requirements, including the security of exchanges of information, are the subject of policy development and compliance audits (see 06.g) consistent with relevant legislation. Cryptography must be used to protect the confidentiality and integrity of remote access sessions to the internal network and to external systems.

f. ***Monitoring***. Monitoring is a right, but not a duty, of the CH IT Security Office. Monitoring includes without limitation reviewing Internet sites visited, reviewing material downloaded/uploaded by Users to/from the Internet, and reviewing e-mail sent and received by Users. This may be done at any time and without prior notice to Users. Reasons for review include but are not limited to, preventing or investigating allegations of abuse, assuring compliance with copyright laws, or complying with legal or regulatory requests for information.

g. ***Circumventing Established Security***. Users may not attempt to circumvent CH' data protection measures or attempt to uncover security loopholes. Users may not gain or attempt to gain unauthorized access to restricted areas or files on CH Resources. Users should not tamper with any software protections or restrictions placed on computer applications, files or directories.

h. ***Encryption***. Users sending emails containing CH Patient Protected Health Information (PHI) as defined by HIPAA and HITECH, or other confidential or sensitive information to non-CH email addresses must encrypt the data using an acceptable method of encryption, approved by CH IT's Information Security. For users of CH email system, encryption is triggered by including "[secure]" anywhere in the *Subject:* line of an outbound CH email. Additional details and instructions may be found on the CH Intranet under the 'Links' – 'Job Aids' section.

i. ***Transmission of Files Containing Patient Information***. The transmission outside of CH of files containing CH PHI must be coordinated through the CH IT Information Security Department. If appropriate, the Information Security Department may allow minimal sensitive information to be e-mailed if it has been encrypted utilizing an acceptable technology as established by CH regulations. Contact the IT Info Security group for appropriate and approved transmission methods.

j. ***Sending Email to Verified Addresses***. You must verify that the email address to which you are sending CH information is correct. It is generally safer to 'reply to' an address rather than typing the address yourself. Whenever possible the encryption discussed in section 5.g should be employed.

6. **Viruses**
    a. ***Virus Detection***. Viruses can cause substantial damage to computer systems. Each User is responsible for taking reasonable precautions to ensure he or she does not introduce viruses into the CH Environment. To that end, Users should not disable virus protection software installed on CH Resources. Users should comply with virus software update announcements as required, and report suspected virus activity to their IT support group and their CH contact, or the CH Service Desk as soon as possible.

7. **Intellectual Property Rights**

    a. Except for rights that have been granted to the User pursuant to any End User License Agreement between CH and the User, any information developed or compiled by the User, including documents such as writings, diagrams, spreadsheets, databases, regardless of form and any invention, discovery, development, modification, system, program, or design that results from the use of CH Environment by the User shall be the exclusive property of CH.

8. **Malicious Destruction of CH Software/Hardware**

    a. CH has considerable investments in software and hardware to provide the environment needed by the employees. Users shall not maliciously destroy or otherwise damage/delete any software licensed to or owned by, or any hardware owned, leased, or otherwise in the possession of CH. Any such damage or destruction shall subject the User to disciplinary action under this Policy. In addition, CH reserves the right to seek compensation through legal action for any damages maliciously caused by the User.

9. **Incident Response**

    a. Users must immediately report to their CH contact, or the CH Service Desk, the CISO or his or her designee any suspected or confirmed security incident. This would include, but not be limited to, a computer virus, breach of security, or security weakness, loss or disclosure of data, or any unauthorized access or use of data.

ADDENDUM TO ACCEPTABLE USE POLICY FOR REMOTE WORK

GENERAL STATEMENT of PURPOSE

The purpose of this addendum to the Acceptable Use Policy is to ensure all Catholic Health employees, consultants and Affiliate Practice staff that have been approved for *remote work status* understand their responsibilities for handling and accessing PHI/PII on their own devices or devices delivered to them by CHS.

PROCEDURE/GUIDELINES

Catholic Health employees, vendors, consultants, and non-employees who have requested and have been approved for remote access must be required to consent to the procedural and confidentiality language in this agreement.

All remote users are required to follow and adhere to Catholic Health Services policies and procedures to protect unauthorized access to data and systems. These procedures will be enforced by Catholic Health Services through automated processes, whenever possible, such as terminating a VPN session after a period of inactivity.

Remote access to Catholic Health Services' network requires additional controls such as strong authentication with two factor or risk-based authentication, and encryption depending on the method of access.

Logging, monitoring, and reporting tools will be used by Catholic Health Services to manage remote access usage when possible.

Remote Access Data Protections

Catholic Health Services prohibits the following:

- Cut, copy or pasting PHI/PII to any device or media.
- Printing CHS or CHS controlled PHI/PII from their device or a CHS device for the duration of this temporary arrangement.
- Using USB for data transfer.
- Transferring PHI/PII via their non CHS email
- Leaving their device unattended while accessing or connected to any CHS system or environment that may contain PHI/PII

User Responsibilities

It is the user's responsibility to follow and adhere to the outlined safeguards in this addendum.

- Never leave a remote access session unattended. Lock your computer (by pressing Ctrl-Alt-Delete) or disconnect from the Catholic Health Services network by logging off of your session.
- Never let another person use your computer or device while connected to the Catholic Health Services network.

POLICY AUTHORITY/ENFORCEMENT

The CH CISO has general responsibility for implementation of this policy.

Anyone who knows or has reason to believe that another person has violated this policy should report the matter promptly in accordance with applicable policy and procedure. All reported matters will be investigated, and, where appropriate, steps will be taken to remedy the situation. Where possible, CH will make every effort to handle the reported matter confidentially.

EXCEPTIONS

Exceptions to this policy can be made with written approval of the CH Chief Digital Information Officer (CDIO) or the Chief Information Security Officer (CISO).

TERMINATION

Upon termination of a User with access to CH Resources, the CH contact or the CH Service Desk must be notified immediately in order to de-provision all access for that user.

Upon termination of agreement, or any other termination of access rights, all programs, files, hardware or any other data defined as intellectual property, must be returned to CH, and any further access to CH systems is strictly prohibited.

REVIEW OF POLICY

In the event that a significant regulatory change occurs, the policy will be reviewed and updated as needed. The policy will be reviewed periodically to determine its effectiveness in complying with the HIPAA Security Regulations, as well as meeting business needs

APPROVED BY:

Michael Mainiero, SVP, Chief Digital & Information Officer
Chief Information Security Officer

Catholic Health

Affiliate Practice Information Acceptable Use Policy Acknowledgment

All users of Catholic Health (CH) network and system resources are expected to adhere to the security policies, procedures, and standards of CH that have been established to support its business processes. A violation of any of the policies, procedures, and standards established pursuant to the CH Information Acceptable Use Policy, or any policy referred to by this agreement, may result in disciplinary action. Disciplinary action may include without limitation, verbal or written reprimand, termination of agreement and/or appropriate legal action.

I have read and understand the CH Information Acceptable Use Agreement, and agree to comply with the policies set forth. I also consent to periodic monitoring of electronic communications including e-mail, as well as any information stored by me on any CH system, as CH management deems necessary.

Where the Signer of this Acknowledgement is an employee of an Affiliate Practice or organizational representative under contract or Agreement with CH, the Signer agrees that it is the responsibility of the Affiliate Practice Company or organization to provide appropriate training to all their employees and agents who will access CH resources.

Signed: _____ Date: _____

Print Name: _____ Job Title: _____

Affiliate Practice: _____

Please retain the attached policy for future reference. Signed acknowledgements by Affiliate Practice employees will be retained by the CH Chief Information Security Office or its designee and kept on file.