NON-EMPLOYEE ACCEPTABLE USE OF INFORMATION SYSTEMS AND EQUIPMENT

This agreement outlines terms regarding the acceptable uses of Fallon Health's Confidential Information, Information Systems, and Equipment by certain contractors, consultants, and personnel affiliated with third party contracts (hereinafter collectively referred to as Users) and your responsibilities with respect to using Confidential Information, Information Systems, and Equipment.

Confidential Information is information related to Fallon Health's business that it maintains in confidence for business, legal, and/or contractual reasons. It is information whose unauthorized disclosure could adversely impact Fallon Health or its employees, members, partners, vendors, providers, or other similar persons or entities. Confidential Information includes:

Proprietary Business Information means non-public knowledge or information concerning Fallon Health's businesses, strategies, operations, financial affairs, organizational matters, personnel matters, business and marketing plans, products, processes, software systems, policies, ideas, trade secrets and technical know-how that is confidential or proprietary in nature;

Protected Health Information (PHI) means individually identifiable health information that is transmitted or maintained in any form or medium;

Personal Information (PI) and Private Information as those terms are defined by MA and NY state law; Payment Card Information (PCI) means credit card numbers and other financial information. This includes:

- Any information on the front of the credit card (or PAN);
- Sensitive authentication data (during credit cardholder processing);
- Any contents of any track on a credit card (the magnetic stripe);
- The card verification code (CVV/CID);
- Personal Identification Numbers (PINs).

Information Systems (referred to as "Systems") are platforms, networks, operating systems, servers, applications, and databases that are owned, maintained, or controlled by Fallon Health; or that are owned, maintained, or controlled by a third party, such as a provider or a business associate, and to which Fallon Health users have been provided access.

Equipment are telephones, mobile phones, personal computers, laptops and other mobile computing devices that are owned, leased, maintained, or controlled by Fallon Health.

CONFIDENTIALITY OBLIGATIONS

You may learn information about Fallon Health's members, employees, and/or business practices that are confidential in nature. You have an obligation to protect Confidential Information from inappropriate use and disclosure during and after your affiliation with Fallon Health. You should not consider your use of or access to any Confidential Information private. Fallon Health reserves the right to monitor all use of and access to Confidential Information.

You agree to:

- Use and disclose Confidential Information according to the contract you have or the company you work for has with Fallon Health.
- Access Confidential Information, including PHI, only for legitimate business purposes. You are prohibited from accessing, using, or disclosing Confidential Information for non-work related purposes and will not attempt to gain access to organization information systems containing sensitive information for which you have not been given proper authorization. For example, you cannot look up your own PHI or look up the PHI of co-workers, friends, family members, public figures, or any other person for personal reasons or out of curiosity.
- Only utilize devices (including smartphones, tablets, PCs, and the like) that have been approved by your employer and/or contract for use in conducting business with Fallon Health. Such use must be consistent with all aspects of this Agreement.
- Disclose Confidential Information only to those individuals with a need-to-know and only to those individuals who have approved access. If you have any questions as to who has approved access to such information, you will seek assistance from your manager or the primary business contact regarding your employer's contract.
- Treat any information pertaining to or obtained from providers or business associates of Fallon Health as confidential.
- Not disclose Confidential Information to an additional third party without the expressed, written consent of Fallon Health.
- Discuss Confidential Information discreetly and in private areas.
- Use reasonable safeguards to protect Confidential Information in any form, including paper, against damage, theft and unauthorized access.
- Return any Confidential Information of which you are in possession to Fallon Health or your employer at the termination of your employment. Immediately report any unauthorized access, use, or disclosure of Confidential Information to Fallon Health's Privacy Officer.

ACCEPTABLE USE OBLIGATIONS

You are permitted to use Fallon Health's Systems and Equipment only for business purposes and only as necessary to perform job functions and responsibilities set forth in your or your employer's contract with Fallon Health.

You should not consider use of Systems and Equipment confidential and/or private. Fallon Health reserves the right to monitor use of its Systems and Equipment. All electronic messages composed, sent, or received on the Fallon Health network are the property of the company.

GENERAL RESPONSIBILITIES

You are responsible for:

- Using and accessing Fallon Health Systems and Equipment as necessary for job related purposes and only as authorized.
- Safeguarding Fallon Health Systems and Equipment from damage, theft, and unauthorized use.
- Safeguarding user IDs and passwords, using them only as authorized, and not disclosing them to or sharing them with anyone including your supervisor and/or administrative assistant.
- Creating passwords that are not based on something that can be easily guessed or obtained using personal information (e.g. names, favorite sports team, etc.).
- Complying with all pertinent licenses, copyrights (including print, audio, and video), and contracts.
- Notifying the Fallon Health IT Helpdesk immediately of any suspected or actual security violations/incidents.
- Using only secure (e.g. encrypted) methods of transmitting Fallon Health Confidential Information.
- Following established process to save Confidential Information only to storage devices/media pertinent to the terms set forth in your company's agreement with Fallon Health.
- Reporting the loss, theft, or inappropriate use of organization access credentials (e.g. passwords, key cards or security tokens) to IT.
- Activate workstation locking software whenever you leave your workstation unattended, and log off from or lock their workstation(s) when their shifts are complete.

You are prohibited from:

- Using Fallon Health Systems and Equipment in any of the following ways or for the following purposes: sending unsolicited email messages (spam) and chain letters, gambling, for personal gain, in any way that is offensive, disruptive, harmful, illegal under local, state, federal or international law, in violation of anti-harassment and/or discrimination laws, or could be construed by another employee as harassing or discriminatory. This includes home computers.
- Downloading or saving Confidential Information to equipment or cloud not specifically authorized by Fallon Health including laptops, mobile devices, portable storage devices and cloud/file sharing services that is not relevant to the terms of your employer's engagement with Fallon Health.
- You are prohibited from emailing Fallon Health Confidential Information to a personal email address/account.
- Adding unapproved software, components, or devices (e.g. thumb drives, cameras, etc.) to Fallon Health Systems and/or Equipment without explicit approval from the Information Security Officer.
- Purposely introducing malicious programs into Fallon Health Systems, modifying configuration files without authorization, removing software, or knowingly executing a program that may hamper normal activities unless authorized by the Information Security Officer.
- Implementing procedures, software, components, or devices that bypass the security controls currently in place in the Fallon Health environment.
- Avoiding or disabling any of the information security measures of any host, network or

account without approval from the Fallon Health Information Security Officer.

- Using personal devices (e.g. smartphones) for the recording of activity at or on behalf of Fallon Health as it may result in the accidental leakage of Fallon Health Confidential Information.
- Engaging in other behavior not mentioned above that is likely to result in a loss of Fallon Health's information confidentiality, integrity, or availability.
- Transmitting of confidential information by text messaging technologies (e.g. SMS/Text). All exceptions must be approved by the Information Security Officer.
- Taking equipment (not including mobile devices and removable media), information and software off site without prior authorization by IT.
- Attempting to gain physical access to secure areas for which you have not been given appropriate authorization.
- Utilizing photographic, video, audio, or other recording equipment in secure areas. Exceptions will be granted for monitoring the organization's data centers.
- Setting up your own networks, network links (such as routing via a cellular device) and wireless access.

Special Requirements for Consultants, Contractors and Third Parties who Access Fallon Health's Information Resources via Equipment that was not issued by Fallon Health and/or access Fallon Health's Information Resources remotely

In addition to acknowledging the above Confidentiality and Acceptable Use obligations, you understand that the above applies to you when you access Fallon Health's network and Confidential Information from your own equipment and/or remotely. If you are working from a remote location, you understand that you are personally responsible for the security of your work area. You understand you are responsible for protecting Fallon Health Confidential Information from intentional, unintentional, incidental or inappropriate use or access by family, friends, or other unauthorized parties. Use of Confidential Information at home must be approved by your supervisor.

You agree to:

- Print Confidential Information only when necessary and dispose of paper documents and other electronic storage devices (e.g. disks, USB drives) by shredding them or bringing them into Fallon Health for disposal.
- Have antivirus software installed and up-to-date virus definitions on the computer or portable device(s) that you use to access Fallon Health's Information Resources.
- Maintain the physical security of any equipment not issued by Fallon Health you use to access Fallon Health's information resources, such as locking/otherwise securing such equipment when it is not in use, and to report to Fallon Health immediately if such equipment is lost or stolen or you suspect unauthorized access to Fallon Health's information resources via your own equipment. Workstations will be handled as carry-on (hand) baggage on public transport. They will be concealed and/or locked when in private transport (e.g., locked in the trunk of an automobile) when not in use.
- Permit Fallon Health to monitor and search the equipment not issued by Fallon Health (e.g. your PC, laptop, mobile devices, and any other portable devices) you use to access Fallon Health's information resources as necessary to respond to or investigate an actual or alleged security event, security incident, or breach of privacy.

Special Requirements for Consultants, Contractors and Third Parties who Access Fallon Health's Information Resources utilizing highly privileged (e.g. admin/root-level) Accounts

You understand that privileged accounts are to be used for system administrative functions only, that additional care must be practiced when using these accounts, and that accessing data or systems for which you have not been authorized is a violation of this Agreement.

I have read, understand and agree with the terms set forth in this Agreement. I understand that a breach of confidentiality of Confidential Information may cause irreparable harm to Fallon Health. I understand that Fallon Health performs periodic monitoring of my use of Systems, Confidential Information, and/or Equipment. I understand that I am responsible for complying with this Confidentiality and Acceptable Use Agreement and that any violation may result in limitations on my use and/or access to Confidential Information, Systems, or Equipment. I understand that a violation of this Agreement may also result in other disciplinary action, up to and including termination of the contract I have, or my company has, with Fallon Health. In addition, Fallon Health may take legal action to address and remedy any violations of this Confidentiality and Acceptable Use Agreement as appropriate. Fallon Health reserves the right to immediately revoke access to Fallon Health Information Resources at any time that a risk in continued use of said systems is perceived.

I agree to be responsible for the equipment or property issued to me. I will follow this Agreement and any Fallon Health policies while using this equipment. Upon separation from Fallon Health, I will return item(s) issued to me in proper working order within seven (7) business days. I acknowledge I am responsible for damages to any item (excluding normal wear and tear) while assigned to me, and that I am responsible for items not returned to Fallon Health for whatever reason.

I understand and acknowledge that nothing in this Confidentiality and Acceptable Use Agreement constitutes a contract for employment for any specific term or sets forth any binding promises or obligations on the part of Fallon Health with respect to the terms and conditions of my or my employer's affiliation with Fallon Health. I understand that my duty to maintain confidentiality continues even after my separation from this engagement.

Signature	Name (Print)
Title	Email Address

Name of Consulting/Contracting Company, if applicable:

_____

Procedure/Process #: 101.01.02PR	**Original date:**	02/23/2015
	Revision date(s):	02/23/2015, 02/05/2016, 03/10/2017, 02/27/2018, 1/27/2019, 2/24/2022
	Review date(s):	3/17/2020, 4/21/2021