OneCare Vermont

Policy Number &Title:	07-03 Privacy and Security Policy
Responsible Department/s:	Compliance
Author	Gregory Daniels
Original Implementation Date	September 23, 2013
Date Reviewed/Revised	October 1, 2019
Next Review Date	October 1, 2020

PART I: PRIVACY POLICY

Section 1 GENERAL RULES

1.1 PURPOSE

OneCare Vermont, ("OneCare" or "ACO"), a Limited Liability Corporation ("LLC") was formed to: (i) participate in cost savings and other arrangements with government programs, commercial insurers and other payers; (ii) develop a network of health care providers for the delivery of health care services according to applicable rules, regulations and contractual obligations for the purpose of improving the quality and efficiency of health care and the patient care experience; (iii) promote evidence-based medicine, patient engagement, reporting on quality and cost, and care coordination and distribution of shared savings, and (iv) engage in other similar or related activities.

So that it may perform these functions, Payers, Participating and Preferred Providers (individually and together "Providers"), and Collaborators (collectively referred to as the "OneCare Network" or "Network") share various types of data and protected health information ("PHI"), as defined under HIPAA, with OneCare. OneCare analyzes this data and PHI and uses it to promote accountability for patient populations, improved care coordination between Providers and their patients, and to encourage investment in infrastructure and the redesign of the care processes to achieve high quality and efficient delivery of services.

OneCare's Participating and Preferred Providers have designated themselves an organized health care arrangement ("OHCA") for the purpose of facilitating the use and disclosure of PHI among them for treatment and health care operations purposes, or as otherwise permitted under the HIPAA Privacy Rule ("HIPAA"), including the implementing Privacy and Security Rules.

The purpose of this Privacy and Security Policy ("Policy") is to provide standards and guidance to OneCare's Board of Managers and Workforce, the Network, Regional Clinician Representatives ("RCRs"), Subcontractors, Vendors, and Awardees regarding the appropriate use or disclose of PHI in OneCare's control and possession. This Policy, together with OneCare's Data Use Policy, has been created to ensure that OneCare manages PHI and other data in accordance with any applicable federal and state privacy laws and in compliance with any contractual obligations with Payers.

1.2 POLICY STATEMENT

It is the policy of OneCare, as a Business Associate ("BA") of its Participants and Preferred Providers, to maintain the confidentiality, integrity, and availability of the PHI of its Participants' patients in accordance with the HIPAA Privacy Rule, its contractual obligations, and applicable privacy laws. OneCare's Board of Managers, Workforce, Participants, Preferred Providers, Collaborators, Regional Clinician Representatives, Subcontractors, and Vendors are required to comply with this policy when accessing or using PHI in OneCare's possession. OneCare may only use and disclose PHI in accordance with contractual obligations and applicable privacy laws.

1.3 DEFINITIONS

The terms used in this part of the Policy shall have the same meaning as those terms as defined under the Privacy and Security Rules of the Administrative Simplification provisions of the federal Health Insurance

Portability and Accountability Act of 1996 ("HIPAA"), Title XIII of the Health Information Technology for Economic and Clinical Health Act ("HITECH"), the American Recovery and Reinvestment Act ("ARRA"), Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule"), and the rules adopted pursuant to HITECH (collectively hereinafter referred to as "HIPAA").

1.4 STATE LAWS

This Policy is intended to comply with applicable state laws affecting OneCare's use and disclosure of PHI.

Section 2 OTHER LIMITATIONS AND RESTRICTIONS

2.1 MINIMUM NECESSARY STANDARD

OneCare will make all reasonable efforts to use, disclose, and request of other covered entities the minimum PHI necessary to accomplish the intended purpose of the use, disclosure or request.

2.2 VERIFICATION OF IDENTITY AND AUTHORITY

Prior to disclosures permitted by this Policy, OneCare will verify the identity of a person requesting PHI and the authority of any such person to have access to PHI if the identity of such person is not already known to OneCare.

2.3 COMPLIANCE WITH NOTICES OF PRIVACY PRACTICES AND REQUESTS FOR RESTRICTIONS AND CONFIDENTIAL TREATMENT

To the extent that a covered entity Participant has specifically instructed OneCare of a limitation contained in their notice of privacy practices or a restriction on how PHI regarding an attributed patient may be used or disclosed, OneCare will, if possible, limit its use or disclosure of PHI received from that Participant in accordance with such limitation or restriction. OneCare shall also discontinue the permitted use and disclosure of a patient's PHI if the patient has affirmatively opted-out of data sharing.

Section 3 PERMITTED USES & DISCLOSURES FOR BUSINESS OPERATIONS

3.1 TREATMENT, PAYMENT & HEALTH CARE OPERATIONS

OneCare may use or disclose PHI of its Participants' patients for Accountable Care Organization Activities "ACO Activities") purposes as described in agreements with its Participants. Generally, OneCare uses and disclosures will be for treatment purposes in connection with care coordination and for health care operations purposes in connection with ACO quality and performance reporting.

3.2 SUBCONTRACTORS

OneCare may use subcontractor(s) to perform certain services for OneCare that may require it to access or use PHI. These subcontractors are required to enter into a subcontractor Business Associate Agreement ("BAA") with OneCare that complies with HIPAA prior to receiving access to any PHI in OneCare's possession or control.

Any subcontractor that releases information to a "next level" subcontractor will be required to enter into a contractual agreement with such subcontractor binding it to the same restrictions regarding use of PHI as apply to OneCare and the original subcontractor.

3.3 DISCLOSURES OUTSIDE OF ACCOUNTABLE CARE ORGANIZATION ACTIVITIES

As an accountable care organization that acts as a business associate to its Participants, OneCare is not likely to receive requests for the use or disclosure of PHI outside the scope of ACO Activities. If OneCare does receive a request(s) for the use or disclosure of PHI outside of ACO Activities, OneCare's Compliance & Privacy Officer, or Legal Counsel, will communicate and cooperate with the relevant covered entity source of the requested PHI regarding proper use or disclosure of the PHI prior to any such use or disclosure. OneCare will comply with any obligation under HIPAA, its contractual obligations with Payers, or any applicable privacy laws to disclose the requested PHI. OneCare will maintain a log and accounting of such uses and disclosures of PHI outside of ACO Activities.

3.4 OTHER PERMITTED AND INCIDENTAL DISCLOSURES

OneCare may disclose PHI for certain internal uses, in emergency situations, for disaster relief recovery, and as incidental to other disclosures as permitted under HIPAA.

3.5 DE-IDENTIFIED PROTECTED HEALTH INFORMATION

Health information that is not individually identifiable and meets the definition of de-identified information under HIPAA is not subject to this Policy. De-identified information may be used by OneCare as authorized by the any relevant Data Use Agreement between OneCare and the covered-entity source of that information and in compliance with OneCare's Data Use Policy.

Section 4 REQUIRED DISCLOSURES

4.1 REQUIRED DISCLOSURES TO THE INDIVIDUAL

OneCare will refer any request for disclosure of health information by an individual to the relevant covered-entity Participant(s) or Preferred Providers, or the relevant Payer. OneCare will cooperate with Participant(s), Preferred Providers, and Payers to fulfill any reasonable and permissible disclosure request from an individual they cannot fulfill. OneCare will disclose such information directly to the individual making the request if required to do so under HIPAA or other applicable law. OneCare may refuse to comply when not so required.

4.2 DISCLOSURES TO THE SECRETARY

OneCare will release health information to the Secretary of the US Agency of Health and Human Services ("HHS"), or any other federal or state government entity with regulatory oversight authority over OneCare, when required to do so under HIPAA or other applicable law.

Section 5 OTHER USES AND DISCLOSURES PERMITTED BY LAW

OneCare may use or disclose PHI to the extent that such use or disclosure complies with HIPAA or any other applicable law. OneCare may disclose PHI under the following circumstances: for public health activities; in response to requests from health oversight agencies; in response to orders or subpoenas issued in accordance with judicial or administrative proceedings; in relation to serious threats to health or safety; in response to discovery requests in workers' compensation matters; in response to qualifying requests related to whistleblowers and victims of crime. All such requests or demands will be reviewed, authorized, and documented by OneCare's Compliance & Privacy Officer or Legal Counsel prior to disclosure.

Section 6 PRIVACY RIGHTS

Under HIPAA, patients have certain rights to access, amend, request restriction or confidentiality of, and/or obtain accountings of disclosures of their health information. OneCare will direct request(s) by an individual(s) to perform such action(s) to the relevant Participant, Preferred Provider, or Payer. Where OneCare's information systems are implicated by the requested action, OneCare will cooperate with to the extent it is able to accomplish the requested action.

PART II SECURITY POLICY

Section 1 ADMINISTRATIVE SAFEGUARDS

This section of the policy applies to the electronic protected health information ("ePHI") created, received, maintained or transmitted by OneCare which is subject to the Security Rule provisions of the Administrative Simplification Provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the rules and regulations promulgated thereunder, specifically the Security Standards for the Protection of Electronic Protected Health Information ("the Security Rule").

It is the policy of OneCare to maintain the confidentiality, integrity, and availability of all ePHI that OneCare creates, receives, maintains or transmits in accordance with state and federal legal requirements. This policy is intended to satisfy the requirements of the HIPAA Security Rule as it is applied to OneCare.

OneCare uses numerous electronic systems to create, maintain, receive and transmit ePHI, which are provided by and under the control of contracted third parties ("Contractors"). OneCare's Network Participants, Preferred Providers, and Payers ("Covered Entities") also use their own electronic systems to interact with ePHI under OneCare's control. Members of OneCare's workforce and certain Participants and Preferred Providers also use electronic mail systems under the control of University of Vermont Medical Center ("UVMMC"), Dartmouth Hitchcock Medical Center ("DHMC"), and other OneCare Participants to transmit ePHI.

Where applicable, OneCare relies upon the administrative, physical, and technical safeguards maintained by the Contractors and Covered Entities, in conjunction with their security policies and procedures, to fulfill its security obligations under HIPAA. OneCare shall maintain up-to-date copies of the Contractors' and Covered Entities' security policies and procedures to fulfill its security-plan documentation obligations under HIPAA.

1.1 DEFINITIONS

The terms used in this part of the policy shall have the same meaning as those terms are defined under HIPAA.

1.2 DESIGNATION OF SECURITY OFFICER AND DUTIES

OneCare shall designate a Security Officer as responsible for the development, implementation, maintenance, enforcement, and documentation of policies and procedures required by the Security Rule. The Security Officer may delegate such duties and tasks as necessary and permitted to fulfill his or her responsibilities.

1.3 SECURITY MANAGEMENT PROCESS

A. RISK ANALYSIS

Annually - and more frequently if necessary to address new security risks, security incidents, or changes in systems used to create, maintain, receive or transmit ePHI - the Security Officer shall conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by OneCare. For outsourced systems, the Security Officer may complete this analysis by obtaining and reviewing risk analyses performed by the contracted provider of the system and/or its subcontractors. For ePHI accessed or disclosed by OneCare Participants or Preferred Providers as a part of ACO Activities, OneCare relies upon risk analyses performed by Participants, Preferred Providers, or Payers in connection with their own compliance obligations with the Security Rule.

Upon the conclusion of each such review, the Security Officer shall document the risk analysis performed and any new administrative, technical, or physical safeguards identified by the review for implementation.

OneCare shall periodically perform a technical and non-technical evaluation to determine whether these policies and procedures meet the requirements of the Security Rule. This evaluation shall be based initially on the standards implemented under the Security Rule and subsequently in response to environmental or operational changes affecting the security of ePHI.

B. RISK MANAGEMENT

As further described in this policy, OneCare shall implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 45 C.F.R. § 164.306(a).

C. SANCTIONS

All security incidents and complaints of violation of this policy shall be investigated by the Compliance & Privacy Officer in coordination with the Security Officer. Where a violation is confirmed to have resulted from

a failure by a Workforce member to comply with this policy, the Compliance & Privacy Officer and/or Security Officer shall ensure that an appropriate sanction is imposed. Sanctions shall be dependent upon the nature of the compliance failure and may range from training to reinforce the policy or procedure violated up to and including termination of employment.

D. INFORMATION SYSTEM ACTIVITY REVIEW

OneCare shall regularly review records of information system activity, such as system activity reports and audit logs, to assess whether there has been unusual system activity that might indicate a threat to the confidentiality, integrity, or availability of ePHI.

1.4 WORKFORCE SECURITY

OneCare shall grant role-based system access privileges to Workforce members to ensure access to ePHI is limited, to the extent possible given system configurations, to those Workforce members requiring access to a particular system and that such access is limited to the ePHI required to carry out his or her job duties. Role-based access privileges shall be reviewed, determined, and documented from time to time by the Security Officer.

If the job or job duties of a member of OneCare's Workforce change, including termination of employment, the Security Officer shall be notified immediately and the member's access privileges will be modified or terminated accordingly.

1.5 INFORMATION ACCESS MANAGEMENT

Using the role-based access determinations made pursuant to Section 1.4, the Security Officer shall direct the provision of access to ePHI to each Workforce member and business associate. The Security Officer, or his or her delegates, shall document system access authorizations granted to each Workforce member or business associate.

1.6 SECURITY AWARENESS AND TRAINING

The Compliance & Privacy Officer and/or the Security Officer shall provide periodic security awareness training programs and updates to all members of OneCare's Workforce, including management.

To the extent OneCare has direct control of equipment on which ePHI is created, received, transmitted, or stored, OneCare shall implement commercially reasonable measures to protect the information systems and ePHI on such equipment from malicious software. To the extent OneCare uses systems under the control of a third party contractor, OneCare will review and document the reasonable measures employed by those contractors to protect their information systems and the ePHI stored or processed on them from malicious software.

OneCare shall obtain reports of log-in attempts to the information systems used by members of its Workforce and monitor those reports for discrepancies, which shall be investigated by the Security Officer as potential security incidents. OneCare systems shall require the use of unique and strong passwords for each individual user. To ensure authentication of the identity of system users, system users are required to safeguard their passwords and shall not share passwords with other individuals.

1.7. SECURITY INCIDENT PROCEDURE

OneCare shall identify and take responsive actions to safeguard against suspected or known security incidents promptly, and shall mitigate, to the extent practicable, any harmful effects. Any suspected security incident shall be immediately reported to the Security Officer, who shall be responsible for investigating the incident, implementing any required response and mitigation and documenting the incident and its outcome.

1.8 CONTINGENCY PLAN

OneCare shall implement, test and update policies and procedures for responding to emergencies or other

occurrences that damage information systems under the direct control of OneCare and shall obtain contingency, disaster recovery and business continuity plans from the contractors that host and/or support systems that are not under the direct control of OneCare. These contingency plans must contain procedures to create and maintain retrievable exact copies of ePHI from all systems, provide for the restoration of any loss of data and include procedures to enable the continuation of business operations for the protection of the security of ePHI while operating in emergency mode. OneCare, and its outsourcing vendors where the systems are hosted or supported on behalf of OneCare, shall perform periodic testing and revision of contingency plans and assess the relative criticality of specific information systems and data in support of other contingency plan components.

1.9. EVALUATION

On an annual basis, the Security Officer shall perform a technical and nontechnical review of these policies and procedures to determine, based on the Security Rule standards and environmental and operational changes that could affect ePHI to determine whether these policies and procedures meet the requirements of the Security Rule.

1.10. BUSINESS ASSOCIATE AND OTHER CONTRACTS

The Security Officer shall annually review relationships with business associates to ensure that any business associate relationship is accurately defined in the contracts between the business associate and OneCare and that the scope or nature of the relationship has not changed over time. The Security Officer will update, modify or terminate relationships with business associates, as needed, after completion of these reviews.

Section 2 PHYSICAL SAFEGUARDS

2.1 FACILITY ACCESS CONTROLS

OneCare shall limit physical access to information systems under its direct control and the facilities in which they are housed by locating servers and similar equipment on which ePHI is stored in a locked room or data center to which only properly authorized personnel are allowed access to secure the systems against unauthorized physical access, tampering and theft. OneCare shall ensure that similar access controls are employed by the contractors hosting outsourced systems and equipment.

Contingency plans created by OneCare or its outsourcing contractors shall address allowed facility access in support of the restoration of lost data in accordance with the disaster recovery plan and emergency mode operations plan in the event of an emergency.

Access to facilities containing computer equipment on which information systems are loaded, including visitor control, shall be limited based on a person's role and function. OneCare or its outsourcing contractors shall document repairs and modifications to key code access devices, locks and similar physical components of facility security.

2.2 WORKSTATION USE

Regardless of where, how or by whom a system is hosted, OneCare workforce members will access the systems and the ePHI in the systems through a variety of workstations, laptops or mobile devices. Workforce members shall employ procedures designed to minimize the risk of improper access to or disclosure of ePHI when using any workstation or other device. These procedures shall include requiring use of a unique password for access to the system, management of paper containing PHI, use of screen savers or sleep mode functions to obscure screen displays of protected information, device placement or screen orientation and other practices to limit the exposure of PHI.

2.3 WORKSTATION SECURITY

OneCare shall implement physical safeguards for workstations to restrict unauthorized access to ePHI. These physical safeguards can include but should not be limited to passwords, screen savers, locking file cabinets, screen display protections, and secure disposal receptacles. Use of workstations should be limited, to the extent possible, to facilities and facility spaces to which OneCare controls access.

2.4 MEDIA & DEVICE SECURITY

OneCare shall, either directly or through its outsourcing contractors, track the receipt and removal of hardware and electronic media containing ePHI into and out of a facility and within the facility. All ePHI shall be irretrievably removed from hardware and electronic media prior to disposal. All ePHI shall be removed from electronic media before re-use. Prior to re-use of any electronic media containing ePHI, the media shall be sanitized in a manner that complies with guidelines on securing electronic media and would prevent the restoration of the ePHI. OneCare shall maintain, directly or through its outsourcing contractors, a record of the movements of hardware and electronic media and the person accountable therefore. Exact copies of the ePHI databases shall be made prior to the movement of any computer equipment.

Section 3 TECHNICAL SAFEGUARDS

3.1 ACCESS CONTROL

OneCare shall implement technical policies and procedures for information systems that maintain ePHI to limit access to only those persons that have been granted access rights as provided in this Policy. Each workforce member or other person authorized to access an information system shall be assigned a unique user identification name and/or number to identify and track that user's identity. EPHI maintained in information systems shall be accessible during an emergency. Where an automatic log-off feature is available, access to information systems will be terminated after a period of inactivity.

The information systems shall contain features that encrypt and decrypt ePHI. At this time, ePHI contained on the equipment maintained by UVMMC is encrypted when transmitted, but not encrypted at rest. Encryption at rest on this equipment would be unduly expensive at this time and could impact other technical safeguards protecting the ePHI at rest. Additionally, the equipment is currently physically isolated and locked, protected by its own firewall and access to the equipment and the ePHI stored on the equipment is very limited. It is expected that the equipment will be upgraded within the next year to a solution that will more easily allow for encryption of the ePHI.

3.2 AUDIT CONTROLS AND INTEGRITY

OneCare shall utilize technical mechanisms implemented by OneCare or provided by OneCare's outsourcing contractors to record and examine activity in all information systems. OneCare shall protect ePHI from improper alteration or destruction, by the periodic review of system activity and audit trail reports to detect data discrepancies.

3.3 PERSON OR ENTITY

OneCare systems ensure that a person or entity seeking access to ePHI is the person or entity claimed by requiring the use of unique user ID's and passwords and other authentication methodologies for system access.

3.4 TRANSMISSION SECURITY

OneCare shall ensure that its outsourcing contractors implement appropriate technical security measures to guard against unauthorized access to ePHI that is transmitted over an electronic communications network and that they have implemented security measures to ensure that ePHI transmitted electronically is not improperly modified without detection prior to its disposition. EPHI shall be encrypted when appropriate

PART III ADMINISTRATIVE REQUIREMENTS

Section 1 Administrative Process

1.1 COMPLAINT PROCESS

Any complaint raised by an individual, a OneCare Participant, or a member of OneCare's Workforce involving privacy, or security, of PHI or ePHI shall be brought to OneCare's Compliance & Privacy Officer, or its Security Officer, respectively, for investigation, documentation, and - where possible - resolution.

1.2 SANCTIONS

When a privacy violation is confirmed to have resulted from a failure by a workforce member to comply with this Policy, the investigating officer(s) shall ensure that an appropriate sanction is imposed. Sanctions shall be dependent upon the nature of the compliance failure and may range from training to reinforce the policy or procedure violated up to and including termination of employment.

1.3 MITIGATION

To the extent practicable, OneCare will mitigate any harmful effect known to it of a use or disclosure of PHI in violation of this Policy.

1.4 INTIMIDATION AND RETALIATION

OneCare will not take any retaliatory action or attempt to intimidate threaten, coerce, discriminate against, or take other retaliatory action against any individual, workforce member, OneCare Participant or patient for the exercise of any right established, or for participation in any process provided for, by OneCare's policies and procedures, including the filing of a complaint.

1.5 DOCUMENT RETENTION

These policies and procedures and any documents created or maintained in connection with an action, activity or assessment required by these policies shall be maintained in written (or electronic) form for six (6) years from the date of creation or the date when last was in effect, whichever is later.

1.6 BREACH NOTIFICATION

Per the HIPAA Breach Notification Rule, OneCare will cooperate with its covered entity Participants to provide notification following a breach of unsecured protected health information. A "breach" may occur any time PHI is impermissibly acquired, accessed, used or disclosed in a manner that compromises its security or privacy. The Compliance & Privacy Officer and Security Officer must be notified immediately of any suspected breaches. The Compliance & Privacy Officer and Security Officer will investigate any suspected breaches and complaints to determine whether there has been a breach that may require reporting and notification and shall notify affected covered entity Participants of any such potential breach. The Compliance & Privacy Officer and Security Officer, as necessary, will be responsible for coordinating with affected covered entity Participants to provide notifications required by the HIPAA data breach rules or other applicable data breach rules.

Location on Shared Drive: S:\Groups\Managed Care Ops\OneCare Vermont\Policy and Procedures\Policies

Management Approval:

Senior Director, Value Based Care — Date: 10/14/19

Chief Operating Officer (COO) — Date: 10/17/19

Chief Compliance Officer — Date: 10/14/19

Board of Managers Approval: *Requires BOM approval annually if content/substantial changes. If N/A BOM approval every two years.

Chair, OneCare VT Board of Managers — Date: 10/15/19