BlueLoop - The MyCareConnect Foundation

HIPAA Compliance

Table of Contents

I. Summary

Working with Children's Medical Center of Dallas (*Children's*), the web and mobile solutions offered through The MyCareConnect Foundation, aka *BlueLoop*, not only were designed to meet the accepted care protocols of doctors and their staff, but also required HIPAA compliance measures. MyCareConnect.com has implemented security measures and policies sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with HIPAA Security Standards §164.306 as follows:

(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.

(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

(3) Protect against any reasonably anticipated uses or disclosures of such information.

(4) Ensure compliance with this subpart by its workforce.

This document details the administrative, physical and technical safeguards of MyCareConnect.com and BlueLoop as well as the organizational, policies, procedures and documentation requirements for HIPAA compliance (164.308, 164.310, 164.312, 164.314, 164.316). Each HIPAA regulation below has a detailed description of the MCC Response at the beginning in italicized blue font followed by the HIPAA regulation itself.

NOTE: the identifier "MCC" in this document refers to both offerings provided by MyCareConnect, BlueLoop.

II. 164.308 Administrative Safeguards

MCC Response:

Working with Children's Medical Center of Dallas, an assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information using both the patient interface and hospital interface or school nurse interface of MyCareConnect.com was conducted.

Agreement to the terms and conditions for the use of MyCareConnect.com for individuals that sign up for the Patient Interface is required. Other entities, including hospitals, clinics, schools, facilities, agencies and their staff that use the MyCareConnect Hospital Interface, School Nurse Interface, have a separate contract governing the terms and conditions of use. Lastly, MyCareConnect staff is governed by its own policies and procedures.

Patient Interface

An individual that signs up to use the MyCareConnect.com patient interface must agree to the terms and conditions and is thus responsible for certain administrative safeguards including:

1) Authorizing access to their account, including password management.

2) Terminating access to their account as they deem necessary.

An individual set up as an administrator of a patient interface account can add, change or delete access rights through the Caregiver Setup screen within MyCareConnect.com. They are also responsible for login id and password setup and maintenance. It is also the responsibility of the administrator, upon assigning access rights to their account, to require the person(s) to agree to the MCC Terms & Conditions of use found on MyCareConnect.com's homepage.

Hospital /School Nurse Interface

Access to the Hospital or School Nurse Interface is setup by MCC. MCC has a separate contract that governs the terms and conditions of use that covers any individual doctor, hospital, clinic, school or school district personnel. The administrative safeguards, by contract, are governed by the policies of the individual doctor, hospital, clinic or school including:

A) Authorization and/or supervision

B) Workforce clearance procedure

C) Termination procedures

MyCareConnect Staff

Employees of MyCareConnect, llc agree to its policies and adherence to HIPAA Security Standards that cover the confidentiality, integrity, and availability of all electronic protected health information. BlueLoop has administrative interfaces that permit access to every MCC account holder's account information. It is protected by

a login id and password that is changed upon any termination of an MCC employee.

Drew Zodrow, current Chief Technology Officer of MyCareConnect, llc, is the assigned security official responsible for the development and implementation of the policies and procedures related to security management including

A) Security awareness and training

B) Security Incident Procedures

C) Contingency plans

D) Periodic technical and nontechnical evaluations

E) Business associate contracts and other arrangements

The protection of MyCareConnect.com from malicious software is set forth through the contract with Zimcom US Inc., which is the web hosting company for MyCareConnect.com (more detail provided in section 164.312 Technical Safeguards).

Policies, Processes, and Documentation

MyCareConnect LLC has a documented Security Policy which details our internal processes for Risk Analysis, Risk Management, Sanctions, and Information System activity review. This Security Policy also contains MCCs internal procedures for Workforce Security, Access Management, Security Awareness and Training, Incident Management, and Contingency Planning.

HIPAA Regulation

(1) (i) **Standard: Security management process.** Implement policies and procedures to prevent, detect, contain, and correct security violations.

(ii) **Implementation specifications:**

(A) **Risk analysis (Required).** Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.

(B) **Risk management (Required).** Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a).

(C) **Sanction policy (Required).** Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.

(D) **Information system activity review (Required).** Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

(2) **Standard: Assigned security responsibility.** Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.

(3) (i) **Standard: Workforce security.** Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.

(ii) **Implementation specifications:**

(A) **Authorization and/or supervision (Addressable).** Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

(B) **Workforce clearance procedure (Addressable).** Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

(C) T**ermination procedures (Addressable).** Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.

(4) **(i) Standard: Information access management.** Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part. (Detail onboarding process for parents/Children's)

(ii) Implementation specifications:

(A) **Isolating health care clearinghouse functions (Required).** If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.

(B) **Access authorization (Addressable).** Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

(C) **Access establishment and modification (Addressable).** Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

(5) (i) **Standard: Security awareness and training.** Implement a security awareness and training program for all members of its workforce (including management).

(ii) **Implementation specifications. Implement:**

(A) **Security reminders (Addressable).** Periodic security updates.

(B) **Protection from malicious software (Addressable).** Procedures for guarding against, detecting, and reporting malicious software.

(C) **Log-in monitoring (Addressable).** Procedures for monitoring log-in attempts and reporting discrepancies.

(D) **Password management (Addressable).** Procedures for creating, changing, and safeguarding passwords.

(6) (i) **Standard: Security Incident Procedures.** Implement policies and procedures to address security incidents.

(ii) **Implementation Specification: Response and Reporting (Required).** Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

(7) (i) **Standard: Contingency plan.** Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

(ii) **Implementation Specifications:**

(A) **Data backup plan (Required).** Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

(B) **Disaster recovery plan (Required).** Establish (and implement as needed) procedures to restore any loss of data.

(C) **Emergency mode operation plan (Required).** Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

(D) **Testing and revision procedures (Addressable).** Implement procedures for periodic testing and revision of contingency plans.

(E) **Applications and data criticality analysis (Addressable).** Assess the relative criticality of specific applications and data in support of other contingency plan components.

(8) **Standard: Evaluation.** Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.

(b) (1) **Standard: Business associate contracts and other arrangements.** A covered entity, in accordance with §164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected

health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with §164.314(a) that the business associate will appropriately safeguard the information.

III. 164.310 Physical Safeguards

MCC Response:

An assessment of the the physical safeguards and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information was analyzed and addressed from a MyCareConnect.com user perspective.

MyCareConnect, llc: *MCC is responsible physical safeguards for its website infrastructure, which is governed by Service Level Agreements with our web hosting provider, Zimcom Inc., which include:*

A) Contingency Operation: MCC's web hosting provider, Zimcom Inc , guarantees the replacement of failed hardware and hardware components located within their datacenters: (i) servers, firewalls, and load balancers; (ii) attached storage devices; and (iii) network attached storage devices. Hardware repair or replacement is guaranteed to be complete within five hours of problem identification for network attached storage devices and within one hour of problem identification for all other hardware.

All databases are backed up daily (full backup on Mondays and incremental backups each evening) and are stored locally. Two weeks of backups are retained. Therefore, if needed, the databases can be restored to a state as recent as 1 day prior up to as far back as 14 days prior.

B) Facility Security Plan: Zimcom.net servers are located within multiple US datacenters. MyCareConnect runs on servers located in their Cincinnati, Ohio datacenter. Access to the datacenters is subject to security badge access and security video surveillance. The data centers are only accessible by personnel who have passed thorough security/background checks. The data centers offer complete redundancy in power, HVAC, fire suppression, network connectivity, and security.

Account Administrator: *Users of the Patient Interface are responsible for their own physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.*

Hospital or School Nurse Interface Users: *Physical safeguards for hospitals, clinics, schools and their staff are covered under their own policies and procedures including:*

Facility Security Plan

Access Control and Validation Procedures

Workstation Use

Workstation Security

Device and Media Controls including final disposition of electronic protected health information, removal of electronic protected health information from electronic media before the media are made

available for re-use, and records of the movements of hardware and electronic media and any person responsible therefore.

Policies, Processes, and Documentation: *MyCareConnect's Security Policy details our internal processes for Physical Safeguards above.*

HIPAA Regulation

(a) (1) **Standard: Facility access controls.** Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

(2) **Implementation specifications:**

(i) **Contingency operations (Addressable).** Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

(ii) **Facility security plan (Addressable).** Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

(iii) **Access control and validation procedures (Addressable).** Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

(iv) **Maintenance records (Addressable).** Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

(b) **Standard: Workstation use.** Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

(c) **Standard: Workstation security.** Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

(d) (1) **Standard: Device and media controls.** Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

(2) **Implementation specifications:**

(i) **Disposal (Required).** Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is

stored.

(ii) **Media re-use (Required).** Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.

(iii) **Accountability (Addressable).** Maintain a record of the movements of hardware and electronic media and any person responsible therefore.

(iv) **Data backup and storage (Addressable).** Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

IV. 164.312 Technical Safeguards

MCC Response:

MCC has implemented technical policies and procedures that allow access only to those persons that have been granted access rights based on the MCC interface they are using:

Patient Interface

A) Logon ID: *An individual that signs up to use the MyCareConnect.com patient interface has a unique logon id, as does each additional Caregiver that the primary user sets up to allow access to the account. MyCareConnect.com is programmed to only recognize one unique logon per user and sends an error message to anyone attempting to create a duplicate logon id.*

B) Emergency Access: *As detailed in the MCC terms and conditions, during an emergency there is no procedure for obtaining necessary electronic protected health information, instead the individual should immediately contact their doctor or call 911.*

C) Audit Controls: *MCC has Audit controls that cover mechanisms that record and examine activity in MyCareConnect.com that contain or use electronic protected health information.*

Hospital /School Nurse Interface

A) Logon ID: *Hospital/Clinic personnel in order to access the MCC Hospital Interface must use a unique logon id and password assigned to them by the hospital/clinic. Once on MyCareConnect.com, before accessing any patient data, personnel must login to access a specific patient's medical records. That additional logon is set up by the hospital administrator. The purpose of this logon is audit control (see below).*

B) Emergency Access: *As detailed in the MCC terms and conditions, during an emergency there is no procedure for obtaining necessary electronic protected health information, instead the individual should immediately contact their doctor or call 911.*

C) Audit Controls: *MCC records activity in the Hospital Interface by capturing the logon id and time stamp each time a patient record is accessed. MCC captures any activity (add, change, delete) that occurs on the patient record.*

D) Person/entity authentication: *A patient or his/her parent or guardian must initiate logical connection to a Hospital by selecting that Hospital in their patient account. That Hospital will verify the patient (byname and DOB) and accept that patient before any Hospital staff can view or act on the patient's record.*

In order to logically connect to a school, a patient account admin must receive a unique school code from the school nurse, and enter that code into the patient account. Only then will any school

personnel be able to view or act on the patient's record.

E) Transmission Security: *To guard against unauthorized access to electronic protected health information that is being transmitted over the internet, MCC uses the Premium GeoTrust QuickSSL Certificate for its enterprise class 128bit data encryption.*

Policies, Processes, and Documentation: *MyCareConnect's Security Policy details our internal processes for Technical Safeguards above.*

HIPAA Regulation

(a) (1) **Standard: Access control.** Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).

(2) **Implementation specifications:**

(i) **Unique user identification (Required).** Assign a unique name and/or number for identifying and tracking user identity.

(ii) **Emergency access procedure (Required).** Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

(iii) **Automatic logoff (Addressable).** Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

(iv) **Encryption and decryption (Addressable).** Implement a mechanism to encrypt and decrypt electronic protected health information.

(b) **Standard: Audit controls.** Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

(c) (1) **Standard: Integrity.** Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

(2) **Implementation specification: Mechanism to authenticate electronic protected health information (Addressable).** Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

(d) **Standard: Person or entity authentication.** Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

(e) (1) **Standard: Transmission security.** Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

(2) **Implementation specifications:**

(i) **Integrity controls (Addressable).** Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

(ii) **Encryption (Addressable).** Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

V. 164.314 Organizational Requirements

MCC Response:

MyCareConnect, llc has an agreement established with Children's Medical Center of Dallas to cover policies and adherence to HIPAA Security Standards. This agreement (contract) is a chain of trust partner agreement between MCC and Children's, in which both partners agree to electronically exchange data and protect the integrity, confidentiality, and availability of the data exchanged.

Pursuant to 164.314, there are no other arrangements or requirements for group health plans.

HIPAA Regulation

(a) (1) **Standard: Business associate contracts or other arrangements.**

(i) The contract or other arrangement between the covered entity and its business associate required by §164.308(b) must meet the requirements of paragraph (a)(2)(i) or (a)(2)(ii) of this section, as applicable.

(ii) A covered entity is not in compliance with the standards in §164.502(e) and paragraph (a) of this section if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful—

(A) Terminated the contract or arrangement, if feasible; or

(B) If termination is not feasible, reported the problem to the Secretary.

(2) **Implementation specifications (Required).**

(i) Business associate contracts. The contract between a covered entity and a business associate must provide that the business associate will—

(A) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity as required by this subpart;

(B) Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it;

(C) Report to the covered entity any security incident of which it becomes aware;

(D) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.

(ii) **Other arrangements.**

(A) When a covered entity and its business associate are both governmental entities, the covered entity is in compliance with paragraph (a)(1) of this section, if—

(1) It enters into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (a)(2)(i) of this section; or

(2) Other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (a)(2)(i) of this section.

(B) If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate as specified in §160.103 of this subchapter to a covered entity, the covered entity may permit the business associate to create, receive, maintain, or transmit electronic protected health information on its behalf to the extent necessary to comply with the legal mandate without meeting the requirements of paragraph (a)(2)(i) of this section, provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (a)(2)(ii)(A) of this section, and documents the attempt and the reasons that these assurances cannot be obtained.

(C) The covered entity may omit from its other arrangements authorization of the termination of the contract by the covered entity, as required by paragraph (a)(2)(i)(D) of this section if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.

(b) (1) **Standard: Requirements for group health plans.** Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to §164.504(f)(1)(ii) or (iii), or as authorized under §164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.

(2) **Implementation specifications (Required).** The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to—

(i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan;

(ii) Ensure that the adequate separation required by §164.504(f)(2)(iii) is supported by reasonable and appropriate security measures;

(iii) Ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and

(iv) Report to the group health plan any security incident of which it becomes aware.

VI. 164.316 Policies & Procedures and Documentation Requirements

MCC Response:

MyCareConnect, llc has implemented reasonable and appropriate maintenance of its policies and procedures both in electronic and written form. The following requirements are also in effect:

*A) **Time limit.** Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.*

*B) **Availability.** Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.*

*C) **Updates.** As part of its audit process, HIPAA documentation and the associated MCC Internal policies and procedures will be reviewed on an annual basis, or updated as needed in response to environmental or operational changes affecting the security of the electronic protected health information.*

HIPAA Regulation

(a) **Standard: Policies and procedures.** Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in §164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.

(b) (1) **Standard: Documentation.**

(i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and

(ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.

(2) **Implementation specifications:**

(i) **Time limit (Required).** Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

(ii) **Availability (Required).** Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

(iii) **Updates (Required).** Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health

information.

VII. MyCareConnect Communications

Each individual MyCareConnect account is created by an administrator, typically a parent or legal guardian, or the patient themselves. An entity such as a hospital or clinic cannot be setup as an administrator of an individual account.

The administrator of an individual MCC account is responsible for granting access and establishing the permissions of all other caregivers thus ensuring that the sender(s) and receiver(s) of information contained on their MCC account is verified establishing HIPAA compliance for "authentication".

MyCareConnect communications include outbound e-mails and text messages as well as inbound text messaging capabilities. Information contained in these communications cannot be linked to an individual nor include any of the protected health information identifiers (PHI) as follows:

Protected Health Information	MCC Transmitted
Names	First name only & first initial of last name
Geographical data (address, city, county, zip code, etc.)	None
Dates (birth, admission, discharge, etc.)	None
Phone or Fax numbers	None
Electronic mail addresses	None
Social Security Number	None
Medical Record Numbers	None
Health plan beneficiary numbers	None
Account numbers	None
Certificate/license numbers	None
Vehicle identifiers, Serial Numbers, License Plate	None
Device Identifiers and Serial Numbers	None
Web Universal Resource Locators (URLs)	None
Internet Protocol (IP) Address Numbers	None
Biometric Identifiers (Finger, Retinal, Voice Prints, etc.)	None
Full Face Photo Images	None
Any Other Unique Identifying Number, Characteristic	None

Outbound Communications:

A) MCC Patient Interface:

As data is entered into MCC, two forms of communication can occur, an e-mail and/or an e-mail sent to a text message address, both setup by the administrator of the MCC account. The following data is transmitted.

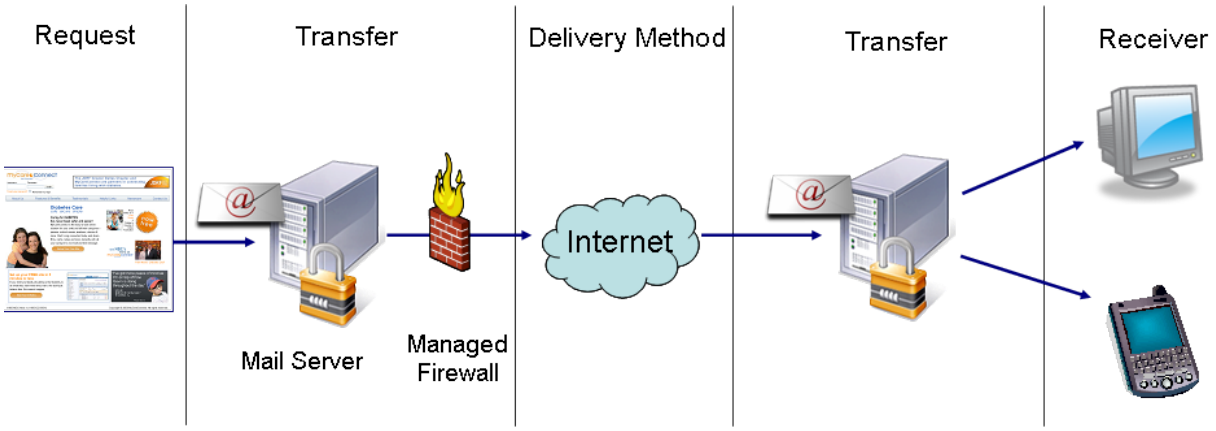
Data Transmitted	Abbreviation	eMail & Text Format
Diabetes: Event	Event:	3 AM Breakfast Post Breakfast Pre AM Exercise AM Snack / Extra AM Test Post AM Exercise Lunch Post Lunch Pre PM Exercise PM Snack / Extra PM Test Post PM Exercise Dinner Post Dinner Bedtime Midnight
Blood Glucose	BG:	###
Carbs	C:	###
Bolus	B:	##.##
Correction Bolus	CB:	##.##
Slow Acting Insulin	Slow:	##.#
Fast Acting Insulin	Fast:	##.#
Ketones	K:	Negative Small Medium Large
Site Change	(no abbrev)	Site Changed
Exercise	Ex:	Low High
Exercise Duration:	Dur:	5 min 10 min 30 min 45 min 1 hr 1 hr 15 min 1 hr 30 min 1 hr 45 min

		2 hrs or more
Notes	N:	{free text 255 Characters}
Date and Time stamp	(no abbrev)	mm/dd/yyyy hh:mm:ss AM/PM
Entered by	By:	Firstname Lastname
Entered by	Updated by:	Firstname Lastname
Patient name	For:	Firstname LastINITIAL
Date	Date:	mm/dd/yyyy
Time	Time:	hh:mm AM/PM
BP Systolic	Systolic:	###
BP Diastolic	Diastolic:	###
Pulse	Heart Rate Pulse:	###
Sodium Intake	Intake-Sodium / Grams:	###
Fluid Intake	Intake-Fluid / Ounces:	###
Vit K	Vitamin K MCG:	###
PT/INR	PT/INR Dose:	###
Weight	Weight:	####
Edema/Swelling	Edema/Swelling:	L-Ankle R-Ankle L&R Ankle L-Foot R-Foot L&R Foot Abdomen
Hypertension / Cardiovascular Event	Event:	Chest Pain Disoriented Dizzy/Light Headed Fall Fatigue Heart Attack Shortness of Breath Stroke Vomiting Other
Asthma Event	Event:	Pre AM Activity Post AM Activity Pre PM Activity Post PM Activity
Inhaler Puffs	Puffs:	#
Nebulizer	Neb:	Y/N

Pre Administration, Left	PreAdmin L:	Clear Wheezing Rales Ronci
Pre Administration, Right	PreAdmin R:	Clear Wheezing Rales Ronci
Post Administration, Left	Post Admin L:	Clear Wheezing Rales Ronci
Post Administration, Right	Post Admin R:	Clear Wheezing Rales Ronci
Peak Flow	Peak Flow:	Green Red Yellow
Oxygen	Oxygen:	Continuous Min
Cognitive Impairment Event	Event:	Agitated Aggressive Confused Depressed Disoriented Emotional Suicidal Wandered Other

* For text messaging, data entered on MyCareConnect in the Notes field are limited to less than 255 characters and vary depending on the size of the entire text message parameters of each carrier.

The MyCareConnect database server and mail server both sit behind a managed firewall providing protection against any intrusion, and within a virtual private network (VPN).



Additionally, the servers use Sophos Antivirus to provide 24x7x365 protection. Sophos uses Behavioral Genotype Protection™ to identify malicious code (Trojan, spyware and other malware) on file servers and delete it before it reaches endpoint computers on the network.

Lastly, messages sent from MCC are sent as "no reply" e-mails and cannot be replied to thus denying access back into MCC.

B) MCC Hospital Interface:

Any communication made through the MCC hospital interface is sent as a notification via e-mail/text to the account administrators. No personal health information (PHI) is transmitted. Instead, the notification informs the account administrator there has been a change to their MCC account, and they will have to securely log on to their MCC account to access their PHI.

Inbound Communications

A) MCC Patient Interface

Wireless data entry, although very rarely used can be sent to MyCareConnect from a wireless device. Messages are sent to wireless@mycareconnect.com in a specific format which is translated to data input in BlueLoop.

Label	Abbreviation (not case sensitive)	Acceptable Results (not case sensitive)
Event	e	**Breakfast**: b, bfast, break, bf **Post Breakfast**: pb, pbfast, pbreak, pbf **Lunch**: l, lunch, lun **Post Lunch**: pl, plunch, plun **Dinner**: d, dinner, din, dnr **Post Dinner**: pd, pdinner, pdin, pdnr **Bedtime**: bed, bedtime, btime, bt **Midnight**: m, mid, mnite, midnight, mnight, mn **3am**: 3, 3am
Blood Glucose	bg	Any whole number between 1 and 600
Carbs	c	Any whole number
Fast Acting Insulin	f	Any number formatted as: x, x.x, x.xx, or x.xxx
Slow Acting Insulin	s	Any number formatted as: x, x.x, x.xx, or x.xxx
Bolus	b	Any number formatted as: x, x.x, x.xx, or x.xxx
Carb Bolus	C	Any number formatted as: x, x.x, x.xx, or x.xxx
Correction Bolus	CB	Any number formatted as: x, x.x, x.xx, or x.xxx
Insulin on Board	IOB	Any number formatted as: x, x.x, x.xx, or x.xxx
Calories	Cal	Any whole number
Exercise Intensity	ExI	Lo, Low, Hi, High, L, H
Exercise Duration	ExD	5, 10, 15, 30, 45, 1, 1.25, 1.5, 1.75, 2, 5m, 10m, 15m, 30m, 45m, 1h, 1.25h, 1.5h, 1.75h, 2h 5min, 10min, 15min, 30min, 45min, 1hr, 1.25hr, 1.5hr, 1.75hr, 2hr 60min, 75min,90min, 105min, 120min 1hr15min, 1hr30min, 1hr45 min 1h15m, 1h30m, 1h45m
Site Change	sc	
Ketones	k	**Negative**: n **Small**: s **Medium**: m **Large**: l
Notes	n	Free text

B) MCC Hospital, Clinic, School, Professional Caregiver Interfaces:

There is no wireless inbound communication through the MCC Hospital, Clinic, School, or Professional Caregiver interfaces.