Children's Medical Group of Saginaw Bay®

**Privacy Policy**

Children's Medical Group ('CMG') considers protecting the privacy of our patients a top priority. This policy contains the policies and procedures of CMG to insure that our patients' health information is protected. All employees must comply with this policy, as well as any other applicable Federal or State law, in order to protect the confidentiality, integrity, and availability of protected health information ('PHI') that is created, received, maintained, or transmitted by CMG. CMG employees must limit disclosure of PHI to the minimum necessary to care for patients.

For the purposes of this policy, PHI refers to any individually identifiable (e.g., information that includes the patient's name, address, birthday, Social Security number, or anything else that could reasonably identify them) health information that relates to either a patients physical or mental health or condition or any provision of health care to the patient. ePHI refers to any of this information stored in electronic form.

The CMG administrator will work with the privacy officer to develop, monitor, enforce and modify these policies and procedures. All employees are encouraged to discuss these policies and procedures with the privacy officer and to make suggestions for improvement. On an annual basis, the privacy officer and CMG Administrator will evaluate CMG to determine compliance with this policy.

**Security Policies and Procedures**

I. **Administrative Safeguards and Policies.**

A. Security Management Process.

1. Risk Analysis. The CMG Administrator will perform a yearly risk analysis, and update policies and procedures accordingly.

2. Risk Management. Based on the risk analysis, the CMG Administrator will implement appropriate security measures in order to reduce the risks.

3. Sanction Policy. Any privacy or compliance violations must be reported to the privacy officer. The CMG Administrator will review the violation and take appropriate disciplinary action and/or make appropriate adjustments to the policies and procedures to prevent future violations.



Version 1, 3/3/03
Version 2, 10/10/12
Version 3, 6/16/13
Version 4, 9/1/14
Version 5, 7/3/15
Version 6, 5/16/2017
Version 7 5/8/2019
Version 8 5/12/2020
Version 9 6/6/2022

4. Information System Review. At least annually, CMG Administrator will review records of information system activity contained in the NextGen Audit Logs for inappropriate use and security incidents.

B. Workforce Security.

1. All CMG staff require access to PHI except the cleaning personnel. Each employee has access to NextGen and individual secured login credentials.

2. On termination or resignation, employees are made inactive in the NextGen, preventing access to PHI.

3. Employees are automatically prompted to change their password every 180 days.

C. Security Awareness and Training.

1. This policy will be reviewed at the time of the privacy officer's annual review in order to determine CMG's compliance with this policy and other applicable law.

2. All CMG employees will be trained as necessary on new privacy policies and procedures.

3. At all times, CMG has updated virus software in place to protect from malicious software. CMG uses Trend Micro Security Agent on every workstation, and their IT vendor verifies updates and functionality.

4. NextGen keeps a log of all system activity which may be accessed if necessary by the CMG Administrator.

D. Security Incident Procedures.

It is the responsibility of every CMG employee to report any known or suspected disclosure of PHI. It is the responsibility of the Privacy Officer to identify and respond to suspected or known security incidents. These incidents are documented, and steps are taken to mitigate the damage and prevent future occurrences.

E. Contingency Plans.

1. Data is backed up nightly and the following morning the data tape is taken offsite.

2. In the event of a system crash, CMG will restore data from backup.

3. In the event of power outage or other computer failure, CMG will use paper records until the system is restored. Upon system restoration, paper records will be entered into the NextGen system and then paper records will be shred.

4. In the event that CMG's building is not usable, CMG will determine an alternate appropriate site to continue to see patients.

5. CMG will periodically test and revise these contingency plans.

## II. **Physical Safeguards.**

### A. Facility Access Controls.

1. All ePHI is kept on password protected computers. The NextGen server is secure and password protected.

2. In the event of an emergency, data will be restored from the backup tape.

3. We do not store any PIN or Security codes for credit card transactions. Any documents containing credit card information is shredded or locked in the front desk cabinet.

### B. Workstation Use/Security.

1. All computer screens with NextGen or PPM will face the employee and should not be left with PHI available if the employee leaves their station. Computers must be locked or logged off if leaving.

2. Employees should make sure they are not displaying another patient's EHR on their computer screen when taking care of a patient. Any written information on a different patient must be protected from parent/patient vision.

C. Device and Media Controls.

1. Any PHI that is being discarded must be shredded.

2. CMG will not keep any ePHI on electronic media, with the exception of the daily backup tape.

3. CMG will ensure that, prior to the movement of any equipment, all PHI is appropriately backed up and stored.
4. CMG's IT contractor ensures that any technology that is destroyed is wiped clean of PHI.

III. **Technical Safeguards.**

A. Access Control.

1. Each CMG employee has unique credentials to access NextGen. Providers with administrative rights have unique workstation credentials.

2. All workstations with NextGen or PPM are programmed to automatically log off after a period of inactivity.

3. NextGen automatically encrypts and decrypts ePHI.

B. Audit Controls.

All NextGen activity is logged within the software, so that in the event of a disclosure or other security activity, the privacy officer may access the audit logs within the NextGen software.

C. Integrity.

1. All CMG employees must **always** verify the patient's date of birth when doing a patient look up. If a parent is calling about their financial account, employees should verify at least one other piece of information (account number, name on account, account address).

2. NextGen automatically authenticates ePHI information.

D. Person or entity authentication.

Parents must provide the child's birth certificate when they enroll in the practice, or in the event that a child enters the practice as a newborn, as soon as they get the certificate. Each parent must show identification to request or access information in person. In order to get information over the phone, parents must provide their social security number to the practice and then provide the last four digits over the phone. The non-parent release form will include a space for a PIN number, so each non-parent who calls can provide their PIN to access their child's health information.

E. Business Associates.

The CMG administrator will execute Business Associate Agreements. The CMG administrator will ensure that all Business Associates appropriately safeguard PHI, and will terminate the agreement if they become aware of material breaches of the Business Associate Agreement. The CMG Administrator will receive annual assurances that the Business Associate is complying with the Business Associate agreement.

**Breaches of PHI**

All CMG personnel are required to report any PHI breach to the CMG privacy officer.

A breach is any disclosure of PHI that compromises its security or privacy. A breach does not include unintentional disclosures to other CMG employees, provided that it does not result in further use or disclosure. It also does not include a disclosure where the unauthorized person would not be able to retain the information. (This includes briefly opening a different patient's record in the exam room, or dropping a chart).

Once the breach is reported, the CMG privacy officer will evaluate the breach to see if a breach notification is required based on CMG's Breach Notification Policy.

**CMG Privacy Policies and Procedures**

1. All patients (including the parent or guardian) will receive a copy of the CMG Privacy Notice and will be asked to sign an Acknowledgement of Receipt form. The form is saved in NextGen. If the parent or guardian refuses to sign, the front desk personnel will sign in the appropriate place on the form. The form will be scanned into the EMR and the privacy

field will be completed along with date signed/refused. If a parent or guardian has more than one child, they may complete all the forms at one time but there must be a separate form for each patient scanned into EMR.

2. Any patient requesting any release of their PHI will complete a Release of Medical Records from CMG form. That form can then be handled following the current Release of Records policy. Any other disclosures, modifications, restrictions, inspections or amendments of PHI that is not part of treatment, payment, or CMG operations must go through the privacy officer. Patients can request a disclosure of all use of their PHI up to three years prior to their request.

3. The privacy officer will review any PHI requests by patients and respond in accordance with our privacy policy and other applicable law within 30 days. Both the requests and response must be in writing.

4. PHI must be obtained by filling out the appropriate paper form. When this information is obtained by phone, no personal identifying information should be revealed. When asking patients about changes to their information, they should have the patient come to the desk or review their information in writing. When calling patients into the examination room, only a first or last name may be used. When discussing PHI with patients over the phone, it must either take place in a private area, or without identifying information.

5. Legal parents or guardians may fill out a 'Non Parent Release Form' to allow a non parent to access a patient's medical information without getting parental consent for each specific encounter. This form allows the parent to describe which type of information the Non-Parent may receive, and is valid until the parent revokes it or the patient turns 18.

6. If anyone other than the legal parent or guardian brings a child to an appointment, then consent to release of medical information regarding that visit is assumed, including information about any referrals or prescriptions that may be necessary.

7. All requests, or documentation related to PHI will be maintained in the patient's electronic or paper chart.

8. Per the above policy, any request for patient information must be in writing. In the event of an emergency record request, CMG employees will confirm the caller's identity by verifying the address and phone number with our information in Patient Template in EMR. Using the record request telephone call template, personnel will document that parent gave

verbal consent to have specific information faxed to ___ site at ___ fax number. Then personnel will document "Info V" meaning that the information was confirmed, including the site and fax number. The record release telephone call can be viewed in the Record release category in NextGen.

**9.** Patients may request restrictions on the release of their PHI in the instance of a medical service for which they pay out of pocket if they submit a written request on or before the procedure.

**10.** The CMG Administrator will maintain a file of training, policies and procedures, privacy notices and violations. The privacy officer handles and maintains a record of all requests from patients. All written requests from patients and the resulting written response from the privacy officer will be kept with the patient chart and will be kept for at least six years. It will not be destroyed sooner if the chart must be maintained under other guidelines for maintaining medical records.

For questions or concerns regarding this policy, please contact our Privacy and Security Officer:
Kelli Roth
(989) 892-5664 or
(989) 793-9982
kelli@cmgsagbay.com



Version 1, 3/3/03
Version 2, 10/10/12
Version 3, 6/16/13
Version 4, 9/1/14
Version 5, 7/3/15
Version 6, 5/16/2017
Version 7 5/8/2019
Version 8 5/12/2020
Version 9 6/6/2022

Children's Medical Group of Saginaw Bay®

## Appendix A: Addressable Requirements

Based on the size of CMG's staff, it is not necessary and appropriate to implement policies and procedures regarding authorization/supervision of ePHI access or determining each individual employee's access to ePHI. All staff members, except cleaning personnel, require access to ePHI. This is because all staff members are involved in patient treatment, payment, or CMG operations.

Since all CMG staff have access to ePHI, it is not necessary and appropriate to implement specific policies and procedures for granting, modifying, documenting, or reviewing access to ePHI.

Because of the size of CMG's staff and facilities, it is not reasonable or necessary to implement policies and procedures to control and validate access to facilities based on role or function.

Because of the size of CMG's staff and facilities, it is not reasonable or necessary to implement policies and procedures to document repairs or modifications to physical components of a facility related to security.

CMG does not keep PHI on electronic media so it is not necessary to maintain a record of their movements.

Many of CMG's PHI protections are included with the NextGen software.

Children's Medical Group of Saginaw Bay®

## Appendix B: Business Associates

CBM Services, Inc.
Function: Collections agency
Contact: Tom Matonican, 989.631.0104 ext. 252,
tom@cbmservices.com BAA Date: 8/18/2014

GBS
Function: NextGen vendor
Contact: Jennifer Ostapiak
BAA Date: 8/20/2014

NextGen Share
Part of EHR
March 2017

Health Wave Connect (Phone Tree)
Function:Patient Reminders for Appts and Pop Health
BAA through existing GBS effective 2016

InstaMed
Credit Card Processing
BAA executed 5/31/2019

PMP Gateway Appriss, Inc
MAPS access
Executed Jan 2018

Michigan Health Connect
Function: HIE Interface
BAA executed 9/19/2013

OTTO Health
Function: Virtual Visits
BAA executed 2/1/2019

Waystar- Formerly Navicure
Function: Claims Processing
BAA executed 7/18/2018