

**EVOLENT HEALTH LLC
POLICY AND PROCEDURE**



POLICY NUMBER: PRW.002.E.KY
 REVISION DATE: March 2018
 PAGE NUMBER: 1 of 7

POLICY TITLE: Confidentiality & Privacy Guidelines – Provider Claims
DEPARTMENT: Provider Claims
ORIGINAL DATE: February 2016

Approver(s): Delilah Foreman, Sr. Manager, Rework Claims

Policy Review Committee Approval Date: September 30, 2019

Product Applicability: mark all applicable products below:

| | |
|----------------------------|---|
| COMMERCIAL | <input type="checkbox"/> HMO <input type="checkbox"/> PPO <i>Products:</i> <input type="checkbox"/> Small <i>Exchange:</i> <input type="checkbox"/> Shop <input type="checkbox"/> All <input type="checkbox"/> Indiv. <input type="checkbox"/> Indiv. <input type="checkbox"/> Large <i>States:</i> <input type="checkbox"/> GA <input type="checkbox"/> MD <input type="checkbox"/> OH <input type="checkbox"/> TX <input type="checkbox"/> _____ |
| GOVERNMENT PROGRAMS | <input type="checkbox"/> MA HMO <input type="checkbox"/> MA C-SNP <input type="checkbox"/> MA D-SNP <input type="checkbox"/> MSSP <input type="checkbox"/> Next Gen ACO <input type="checkbox"/> MA All <input checked="" type="checkbox"/> Medicaid <i>States:</i> <input type="checkbox"/> DC <input checked="" type="checkbox"/> KY <input type="checkbox"/> MD <input type="checkbox"/> _____ |
| OTHER | <input type="checkbox"/> Self-funded/ASO |

Regulatory Requirements: HIPAA Privacy Regulations: 45 CFR Parts 160 and 164 Standards for Privacy and Individually Identifiable Health Information; Final Rule, Kentucky Department for Medicaid Services Contract Section 32.7

Related Documents: Privacy Policy No. CORP.007.E

PURPOSE

Evolut Health (Evolut) collects, processes, transmits, maintains and provides access to substantial amounts of information, much of it sensitive and confidential, about members, employees and providers. This information is used to oversee the delivery of care, compensate healthcare providers, and measure and improve care. In addition, laws, regulations, and accreditation standards that relate to confidentiality and privacy issues must be followed. This policy defines guidelines to protect Members, employees, and providers, privacy and confidentiality process and procedures.

DEFINITIONS

Confidential Information includes, but is not limited to:

- Protected Health Information (defined below)
- Personal information concerning employees, members, and providers

- Practitioner-specific information related to credentialing proceedings, quality reviews, malpractice suits, peer-reviewed determinations, etc.
- Financial information relating to employees, members, providers, contractors, subcontractors, vendors and consultants
- Proprietary business information and trade secrets

De-Identified Information means information from which the following identifiers have been removed or otherwise concealed by a person with appropriate knowledge and experience, and there is no reason to believe that any anticipated recipient of the information could use the information, alone or in combination with other information, to identify an individual:

- Name
- All geographic subdivisions smaller than State level, including street address, city, State, and zip code
- Names of relatives
- Name of employer
- All elements of dates (except year) for dates directly related to the individual
- Telephone numbers
- Fax numbers
- Electronic mail (e-mail) addresses
- Social Security number
- Medical record number
- Health plan member number
- Account number
- Certificate/License number
- Any vehicle or other device serial number
- Web Universal Resource Locator (URL)
- Internet Protocol (IP) address number
- Biometric identifiers (such as voice or finger prints)
- Photographic images
- Any other unique identifying number, characteristic, or code that may be available to an anticipated recipient of the information.

Healthcare Operations means any of the following activities of the covered entity to the extent that the activities are related to covered functions, and any of the following activities of an organized healthcare arrangement in which the covered entity participates:

- Conducting quality assessment and improvement activities or population-based activities relating to improving health or reducing costs, protocol development, case management and care coordination, and related functions that do not

Confidentiality & Privacy Guidelines – Provider Claims

POLICY NUMBER: PRW.002.E.KY

REVISION DATE: March 2018

PAGE NUMBER: 3 of 7

include treatment;

- Reviewing the competence or qualifications of healthcare professionals;
- Underwriting, premium rating, and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits;
- Conducting or arranging for medical review, legal services, and auditing functions;
- Business planning and development;
- Business management and general administrative activities, such as: management activities, customer service, internal grievance resolution, due diligence in connection with the sale of assets, creating de-identified health information, fundraising, and marketing.

Privacy authorization is the mechanism for obtaining consent for the use and disclosure of Protected Health Information (PHI) in instances other than treatment, payment, and healthcare operations.

Protected Health Information (PHI) or Individually Identifiable Health Information, as used in this policy, means health information (including demographic information) collected about an individual that:

- Is received from the individual, the Department for Medicaid Services, a health care provider, another health plan, health care clearinghouse or created by Evolent itself; and
- Relates to the past, present or future physical or mental health or condition of an individual, provision of healthcare to that individual, or the past, present or future payment for the provision of healthcare to the individual, and that identifies or with respect to which there is a reasonable basis to believe the information can be used to identify the individual. [Note: the information could be identifiable either explicitly, by linking health information to an individual's name, or implicitly, by providing information that could be combined with other information to identify the individual, such as a Social Security number, date of birth, etc.]

PHI includes, but it is not limited to, medical records, claims, and utilization management records.

POLICY

It is the policy of Evolent to outline the ways in which confidential information will be protected in the provider claims department and be consistent with 1) applicable federal and state laws and regulations; 2) Evolent's standards of conducting business without collecting or divulging more information than is necessary; and 3) the need to do research and measure quality using aggregated or non-identifiable data whenever

possible.

Provider claims will protect all collected Confidential Information that is used or disclosed in the course of performing job duties. Provider claims has access to certain protected health information that is used to process/reprocess claims and related services for providers. Provider claims staff will use the minimum amount of protected health information necessary to accomplish required job tasks.

All provider claims staff must read and sign a confidentiality agreement and related privacy and confidentiality policies upon hire. Temporary employees, contractors, consultants, or student workers/interns working in the provider claims area must also read and sign the confidentiality agreement and privacy policies. It is the responsibility of the human resources manager and management staff to ensure all permanent and temporary staff signs the confidentiality agreement.

It is not permitted for provider claims staff to use or disclose a member's protected health information for reasons other than to coordinate treatment or facilitate payment and healthcare operations without obtaining a written privacy authorization from the member. Any provider claims employee who receives a request for information that requires a privacy authorization must contact the privacy officer before this information is disclosed. (Please see CORP.007.E)

This policy does not supersede Evolent's policy on Privacy CORP.007. E.

This policy is intended to comply with current state and federal laws and regulations, as well as accreditation standards of the national committee for quality assurance. As such requirements and standards change, this policy will be reviewed at least annually and revised as needed.

PROCEDURE

Access to Data, Files, and Records

All provider claims staff, including the department supervisor, quality auditor, and all other employees has access to member specific information in order to perform job functions.

Provider claims staff is permitted access to necessary departmental systems that contain PHI to coordinate treatment and facilitate payment and healthcare operations.

The provider claims department uses and discloses PHI internally and externally for the purposes of:

Confidentiality & Privacy Guidelines – Provider Claims

POLICY NUMBER: PRW.002.E.KY

REVISION DATE: March 2018

PAGE NUMBER: 5 of 7

- Reviewing provider inquires
- Reversing and reprocessing claims for payment
- Scanning all paper correspondence connected to a claim into departmental systems
- Creating and responding to service forms in connection with reprocessing claims.

The provider claims department requests member medical records from providers and other facilities to obtain information necessary to reprocess claims. Provider claims staff will only request PHI from another entity if they have a demonstrated need to know requirement and may only request the minimum amount of PHI necessary for the specific purpose. The entire medical record is requested only if the entire contents are determined to be necessary. Provider claims staff who receives requests for member information from an outside practitioner, provider or facility must take steps to make sure the information requested and disclosed is only the minimum necessary for the request.

All medical records requested are scanned into the departmental systems upon receipt. Only designated staff is permitted to scan documents into these systems.

Confidentiality and HIPAA guidelines must be followed when scanning all documents that contain PHI.

Committees

Members of the provider claims department may be asked to chair, attend, or supply information for various committees. If a committee consists of members who are not employees, those external members will be asked to read and sign a confidentiality agreement. The confidentiality agreement outlines the committee member's responsibilities for protecting information confidentiality. The confidentiality agreements will be reviewed and signed annually. The nature of some committee discussion requires that member information is not blinded. Whenever possible, member information will be blinded for committee discussion.

General Provider Claims Departmental Privacy and Confidentiality Guidelines

- All faxes sent by this department that contain confidential information will be sent with a confidential cover letter from a fax machine located in a secure area. The sender should take steps to ensure that the intended recipient received the faxed information.
- Information of a confidential nature will not be left unattended or in plain sight in any work area. Confidential information should be removed in a timely fashion from printer output bins, fax machines and copiers. Computers will be turned off

Confidentiality & Privacy Guidelines – Provider Claims

POLICY NUMBER: PRW.002.E.KY

REVISION DATE: March 2018

PAGE NUMBER: 6 of 7

at the close of business each day.

- Any member-related information obtained in connection with performing job responsibilities will not be shared with other associates unless the information is necessary to the performance of the associate’s job duties.
- Confidential information on paper shall be stored in locked file drawers or turned over on an employee’s desk. Other filed information in the provider claims department is stored in a locked area on site. Confidential information on paper that does not need to be saved will be placed in a confidential bin for shredding.
- Communications with providers, hospitals, subcontractors, and other agencies will be limited to the minimum necessary, except for treatment purposes, to accomplish purpose.
- Communications with individuals about whom the protected health information is referring are not limited to minimum necessary.
- The e-mailing of PHI to external entities is not permitted unless adequate levels of encryption are used. Putting “#Secure#” in the subject line of your email will password protect and encrypt PHI.

Sanctions

Any suspected violations of this policy should be reported to the department supervisor and/or director and the privacy officer. If the violation involves accidental or negligent misuse of confidential information, an investigation may be conducted, and progressive disciplinary actions may follow in accordance with human resources guidelines. Intentional misuse of confidential information will not be tolerated and may result in suspension or termination.

RECORD RETENTION

Records Retention for Evolent Health documents, regardless of medium, are provided within the Evolent Health records retention policy and as indicated in CORP.028.E Records Retention Policy and Procedure.

REVIEW HISTORY

| DESCRIPTION OF REVIEW / REVISION | DATE REVISED |
|--|---------------------|
| New Policy | 09/16 |
| Due to dept split, updated according to new dept functions | 03/18 |

Confidentiality & Privacy Guidelines – Provider Claims

POLICY NUMBER: PRW.002.E.KY

REVISION DATE: March 2018

PAGE NUMBER: 7 of 7

| | |
|---------------|------|
| Annual review | 9/19 |
|---------------|------|