

# **Goochland County Department of Fire-Rescue**

## **Health Insurance Portability and Accountability Act (HIPAA)**

### **Privacy Rule Compliance Plan**



# Table of Contents

I. Health Insurance Portability and Accountability Act Definitions .....	4
II. Access, Disclosure, and Security of Protected Health Information .....	6
Role Based Access .....	6
Disclosures of Protected Health Information .....	7
Disclosures to Business Associates .....	8
Disclosures to Law Enforcement.....	8
Miscellaneous Disclosure Situations .....	10
GCFR Requests for PHI .....	12
Incidental Disclosures .....	13
Verbal Security.....	13
Physical Security .....	14
Computer Security.....	15
III. Notice of Privacy Practices.....	16
IV. Medical Records of Employees.....	17
V. Privacy Training .....	18
VI. HIPAA Compliance Officer .....	19
HIPAA Compliance Officer – Principle Responsibilities .....	20
VII. Patient Requests for Protected Health Information .....	21
Procedure for Patient or Authorized Representative Access .....	21
Requests for Amendment to PHI.....	23
Requests for Restriction .....	24
Accounting for Uses and Disclosures of PHI.....	25
VIII. Designated Record Sets .....	26
IX. Complaints and Privacy Breaches .....	27
X. Appendix – Forms .....	28
Notice of Privacy Practices .....	29
Patient Request for Access Form .....	33

Denial of Request for Access to Protected Health Information.....	34
Request for Amendment of Protected Health Information .....	36
Acceptance of Request for Amendment of Protected Health Information .....	37
Denial of Request for Amendment to Protected Health Information .....	38
Patient Accounting Form.....	39
Accounting Log for Disclosures of Protected Health Information .....	40
Patient Request for Restriction Form .....	41
Authorization to Use and Disclose .....	42
Specific Protected Health Information .....	42
Procedure for Filing Complaints About Privacy Practices.....	44
Log for Processing Complaints About Privacy Practices .....	46
Privacy Training Record Form.....	47
List of Designated Privacy Officials .....	48

## I. Health Insurance Portability and Accountability Act Definitions

**Authorized Representative.** Someone who is legally entitled to receive another person's protected health information, such as a parent or legal guardian, an immediate family member of a deceased individual, an executor or administrator of the estate of a deceased individual, or someone who has power of attorney for another person.

**Business Associate.** A person or organization that performs a service for a covered entity that uses or discloses individually identifiable health information including, but not limited to, billing, quality assurance, peer review, and claims processing.

**Covered Entity.** A health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a transaction involving the transmission of information between two entities.

**Direct Treatment Relationship.** Relationship between an individual and a health care provider that is not an indirect treatment relationship.

**Disclosure.** The release, transfer, provision of access to, or divulging in any other manner of information to another entity.

**Health Care.** Care, services, or supplies related to the health of an individual.

**Health Care Operations.** Activities not directly related to treatment or payment such as quality assessment, protocol development, improvement activities, training programs, fraud and abuse detection, and compliance programs.

**Health Care Provider.** Provider of medical or health services and any other person who bills, furnishes or is paid for health care in the normal course of business.

**Health Information.** Any information, oral or recorded in any form or medium, that is created or received by a health care provider and relates to the past, present or future physical or mental health/condition of an individual or the past, present or future payment for health care services provided to an individual.

**Indirect Treatment Relationship.** Relationship between an individual and a health care provider in which the health care provider delivers health care to an individual based on the orders of another health care provider.

**Individually Identifiable Health Information.** Information that is a subset of health information including demographic information and is created or received by a health care provider; relates to the past, present, or future physical or mental health or condition of an individual and identifies the individual, or there is a reasonable basis to believe the information may identify an individual.

***Privacy Rule.*** The Standards for the Privacy of Individually Identifiable Health Information as promulgated by the United States Department of Health and Human Services.

***Protected Health Information.*** Individually identifiable health information that is transmitted by electronic media, or maintained or transmitted in any other form or medium.

***Security Rule.*** The proposed regulations from the United States Department of Health and Human Services addressing the technical and physical safeguarding of protected health information.

***Transaction.*** The transmission of information between two parties to carry out financial or administrative activities related to health care.

***Use.*** The sharing, employment, application, utilization, examination, or analysis of individually identifiable information held within the entity that maintains the information.

## II. Access, Disclosure, and Security of Protected Health Information

### *Role Based Access*

Access to PHI will be limited to those who need access to protected health information (PHI) to carry out their duties. The following describes the specific categories or types of PHI to which such persons need access and the conditions, as appropriate, that would apply to such access.

<b>Job Title</b>	<b>Description of PHI to Be Accessed</b>	<b>Conditions of Access to PHI</b>
EMT (all levels)	<ul style="list-style-type: none"> <li>• Patient information obtained from CADS or ECC</li> <li>• Patient care reports</li> </ul>	May access only as part of completion of a patient event and post-event activities and only while actually on duty.
Direct supervisor or field training officer/Precept or	<ul style="list-style-type: none"> <li>• Patient information obtained from CADS or ECC</li> <li>• Patient care reports</li> </ul>	May access only as part of completion of a patient event and post-event activities, as well as for quality monitoring of activities of direct subordinates.
Performance Improvement Committee	<ul style="list-style-type: none"> <li>• Patient information obtained from CADS or ECC</li> <li>• Patient care reports</li> </ul>	May access only as a part of training and quality management activities. All individually identifiable patient information should be redacted prior to use in training and quality assurance activities.
Chief Level Officers		May access only to the extent necessary to monitor compliance and to accomplish appropriate supervision and management of personnel.
Revenue Recovery Program Manager	<ul style="list-style-type: none"> <li>• Patient information obtained from CADS or ECC</li> <li>• Patient care reports</li> </ul>	May access only to the extent necessary to perform assigned tasks and only during actual work shift.
Designated support staff*	<ul style="list-style-type: none"> <li>• Patient information obtained from CADS or ECC</li> <li>• Patient care reports</li> </ul>	May access only to the extent necessary to perform assigned tasks and only during actual work shift.
County Administrator, Deputies, and Board of Supervisors' members		May be notified and provided only the minimum necessary information needed to carry out the essential duties of governing the County.

\*Designated Support Staff includes those individuals authorized to assist with administrative tasks such as PCR fax transmittal, PCR processing for billing, PCR retrieval (e.g., patient requests or subpoenas), database management, and hardware and software support.

Access to PHI is limited to the above-identified persons only, and to the identified PHI only, based on the GCFR HIPAA Compliance Officer's reasonable determination of the persons or classes of persons who require PHI, and the nature of the health information they require, consistent with their job responsibilities.

Access to a patient's entire file will not be allowed except when provided for in this and other policies and procedures or approved by the HIPAA Compliance Officer.

### ***Disclosures of Protected Health Information***

Members are NOT required to limit disclosure to the minimum amount of information necessary when disclosing PHI to other health care providers for treatment of the patient. This includes doctors, nurses, etc. at the receiving hospital, rescue squad members, any mutual aid provider, fellow crewmembers involved in the call, and any other person involved in the treatment of the patient who has a need to know that patient's PHI.

GCFR members may disclose any PHI about a patient directly to the patient or authorized representative, without concern for any limitation or the minimum necessary provision. In addition, disclosures to others authorized by the patient are exempt from the minimum necessary requirements unless the authorization to disclose PHI is requested by GCFR.

Authorizations received directly from third parties, such as Medicare, or other insurance companies, which direct members to release PHI to those entities are not subject to the minimum necessary standards. For example, if GCFR has a patient's authorization to disclose PHI to Medicare, Medicaid, or another health insurance plan for claim determination purposes, GCFR is permitted to disclose the PHI requested without making any minimum necessary determination.

For all other uses and disclosures of PHI, the minimum necessary rule is likely to apply. A good example is when GCFR conducts quality management activities. This includes, but is not limited to, quality assurance audits, PCR reviews, call critiques, evaluating provider performance, and investigations of problems in clinical care. For example, in most situations, in order to conduct a call review, it is not necessary to disclose certain patient information such as the patient's name, address, or social security number – all PHI of the treated patient. This sensitive information should not be revealed in such cases, or should be redacted or blacked out from the PCR being used as a Q/A example, unless it is needed for the purpose of the review.

Another example of when the minimum necessary rule applies is conducting critical incident stress defusings or debriefings. Revealing patient identifiers during such proceedings is usually unnecessary and should be avoided.

Except as described above or elsewhere in this Plan or GCFR policies and procedures, PHI shall not be disclosed to any person or entity outside the organization. Requests from such persons or entities for access to PHI shall be referred to the Fire-Rescue Administration.

### *Disclosures to Business Associates*

Entities that use PHI to perform a service on behalf of GCFR are considered Business Associates. Disclosures to Business Associates shall follow the guidelines described herein, including the minimum necessary provision, and shall be made only when a valid Business Associate Agreement (BAA) is in place between GCFR and the Business Associate.

Other health care providers with direct treatment relationships with GCFR's patients are not considered Business Associates, and require no BAA in order for PHI to be disclosed for treatment or payment purposes.

Disclosures to Business Associates will be handled by the Fire-Rescue Administration.

### *Disclosures to Law Enforcement*

EMS services and personnel often receive requests from law enforcement officials for PHI. The Privacy Rule does *not* permit the disclosure of PHI to law enforcement officials for purposes of assisting generally in their investigation or building a case against a suspect. For purposes of this section, "officers" refers to any sworn law enforcement official, including police officers and sheriff's deputies.

Field personnel will encounter these disclosure situations under either emergency or non-emergency situations. In non-emergency situations, the requestor shall be referred to the Fire-Rescue Administration. In emergency situations, field personnel should exercise professional judgment in deciding whether a request meets one of the criteria described below and meets the overall intent of HIPAA. In questionable emergency situations, field personnel shall, when feasible, consult a GCFR supervisor (such as a company officer or battalion chief) or the HIPAA Compliance Officer before releasing PHI to law enforcement. Such consultation may be in person, by phone, or by radio.

In all cases when disclosures of PHI to law enforcement are allowed, such disclosures shall include only the minimum necessary information needed for officers to accomplish the task(s) for which the disclosures are allowed.

Disclosures to officers are allowed for specific defined purposes, and may be made in the following circumstances:

1. *Officer as a health care provider.* When the officer is functioning as a care provider, PHI necessary for treatment may be freely exchanged as it may be with any other health care provider.
2. *Disclosures pursuant to a subpoena, court order, or other judicial process.* Such disclosures are normally required by law, but will be handled by the HIPAA Compliance Officer. Field personnel receiving subpoenas for PHI shall forward them promptly to the HIPAA Compliance Officer.



3. *Victims of a crime.* Providers may disclose PHI about a crime victim to an officer if:
  - a. The affected individual agrees to the disclosure, or
  - b. If an individual's agreement cannot be obtained due to the individual's incapacity or other emergency, and if the officer needs the information to determine whether a violation of the law has occurred. The officer must represent that waiting until the patient is capable of agreeing to the disclosure would compromise an immediate law enforcement activity. The officer must also assure the EMS crew that the information will not be used against the victim. If the victim is also a suspect of a crime, only the PHI permitted to be disclosed for a suspect (described in the next paragraph) shall be released. The first responsibility of EMS personnel is to their patient, and they shall use professional judgment in determining whether the disclosure is in the best interests of the patient.
  
4. *Identifying or locating a suspect, fugitive, material witness, or missing person.* Partial PHI may be disclosed to officers in these situations. The content of such disclosures may include only the following information about the patient:
  - a. Name
  - b. Address
  - c. Date and place of birth
  - d. Social security number
  - e. Blood type
  - f. Type of injury
  - g. Date and time of treatment
  - h. Date and time of death, if applicable
  - i. Description of distinguishing physical characteristics such as weight, hair color, eye color, gender, presence or absence of facial hair, scars, and tattoos.
  
5. *Alerting law enforcement to a crime.* PHI may be disclosed to officers if necessary to alert them to:
  - a. The commission and nature of a crime,
  - b. The location of such crime and/or the victims of a crime, and
  - c. The identity, description, and location of the perpetrator of the crime.

This section includes cases where the patient has suffered a wound inflicted by another party with a suspected illegal weapon.

6. *Averting a serious threat to health or safety.* PHI may be disclosed to officers (or other appropriate parties) if:
  - a. The provider, in good faith, believes the PHI's disclosure is necessary to prevent or lessen an imminent threat to health or safety of a person or the public, and
  - b. If the officer (or other appropriate party) to whom the PHI is revealed is able to prevent or lessen the threat.

7. *Crimes on GCFR property.* PHI may be disclosed to officers if the provider believes, in good faith, that the PHI contains evidence of a crime that occurred on GCFR property.
8. *Criminal death investigations.* If there is a suspicion that a death may have resulted from criminal conduct, PHI about the deceased may be disclosed to officers in order to alert them to the possibility of a crime.

### ***Miscellaneous Disclosure Situations***

#### Disclosures Requiring an Opportunity for the Patient to Agree or Object

Certain types of disclosures beyond treatment, payment, and operations are allowed under HIPAA, but require that the patient ordinarily be given an opportunity to verbally agree or object. In these cases, reasonable efforts shall be made to obtain the patient's agreement to disclose the PHI. When the patient is not present, is incapacitated, or is involved in an emergency, providers shall exercise professional judgment and determine whether the disclosure is in the best interests of the patient. If so, then only the minimum necessary PHI may be revealed to accomplish the purpose of the disclosure.

Two scenarios are described here. The first situation, very common, involves family or friends that are involved with the patient's care. PHI directly relevant to such person's involvement may be disclosed. An example would be a spouse present at the scene of an EMS call.

A much less common situation, but possible nonetheless, is for disaster relief purposes. In such cases, PHI may be released to a public entity or private disaster relief organizations (e.g., the Red Cross) for the purposes of assisting in coordinating information about a person's location, general condition, or death in a disaster or mass casualty situation.

#### Disclosures in Response to Communicable Disease Exposures

Virginia law allows certain individuals, including firefighters, EMS providers, law enforcement officials, and laypersons, to be notified of a patient's communicable disease status following exposure of blood or body fluid to mucous membrane or non-intact skin, or following a contaminated needle stick injury. Disclosures may be made as needed for this notification.

Requests for these disclosures shall be referred to the Fire-Rescue Administration for action.

#### Disclosures for Judicial and Administrative Proceedings

PHI may be disclosed in the course of certain judicial or administrative proceedings. Such disclosures may be made in response to a court-ordered subpoena. They may also be made in response to an attorney-generated subpoena, discovery request, or other lawful process, but only if GCFR has obtained satisfactory assurances that reasonable efforts have been made to notify the individual of the request.

Requests for these disclosures shall be referred to the Fire-Rescue Administration for action.

## Disclosures for Research Purposes

PHI disclosure for research purposes shall be made only: 1) if PHI has been appropriately de-identified as required by the Privacy Rule, or 2) with documentation that an Institutional Review Board or privacy board has approved the disclosure in accordance with the Privacy Rule. Disclosures for research purposes shall be limited to the minimum necessary provision described previously.

Requests for such disclosures shall be referred to the Fire-Rescue Administration for action.

## Disclosures to the News Media

Caution is needed when releasing information to the press. Good judgment should be used, and HIPAA's intent considered. The benefit of releasing information to the press should be weighed against the risk of violating HIPAA in the context of the current situation.

As long as no names or other patient identifiers are released, there is generally no problem releasing certain information about an incident to the press if otherwise allowed by law and by department or county policies and procedures.

Here are some scenarios that might arise:

- An MVA with major injuries and/or fatalities: General information such as the number and general nature of injuries or fatalities should be acceptable to release. For example, it could be reported that there were two fatalities, one critical injury who was Med-Flighted, and two minor injuries. Avoid any specific description of the injuries, in the event the press is otherwise able to identify the patient. To provide non-clinical information should be acceptable too, such as the fact a patient was trapped for 30 minutes.
- A fire-related injury or death: The Fire Marshal's role as a fire investigator is a non-health care function of our department (see the next section for details). Any information an investigator obtains in that role is not covered by HIPAA. Therefore, to release that information is not a HIPAA issue. Care should be taken to assure that PHI obtained in GCFR's role as a provider of patient care for the fire casualty is not intermingled with findings released by a Fire Marshal in the role of an investigator.
- Non-fire related incidents at a patient's residence: This probably requires the greatest caution and discretion. The address is self-evident, and that may be enough for the press to identify the patient. If ANY information on the nature and extent of injury is released, regardless of how general it is, it could be construed as PHI if the patient can be identified. For example, for a response for a gunshot wound at a patient's home, GCFR tells the press only that the patient has a gunshot wound and is critical. The press finds out from a neighbor that the homeowner's name is John Smith. The press now announces that John Smith is in critical condition with a gunshot wound. GCFR would be hard-pressed to defend its release of information under HIPAA.

## Disclosures by the Fire Marshal

HIPAA allows covered entities who are single legal entities, and that conduct both covered (i.e., health care) and non-covered functions, to elect to be a “hybrid entity.” This allows “firewalls” to be established between covered and non-covered functions, exempting the non-covered functions from most of HIPAA’s requirements.

The County government is a hybrid entity, and some functions within GCFR are not covered by HIPAA. GCFR has established a firewall between the investigative function of the Fire Marshal’s office and the health care function of the department as a whole. Accordingly, any information on fire casualties obtained by a representative of the Fire Marshal’s office in his/her role as an investigator is beyond the jurisdiction of the HIPAA Privacy Rule.

This firewall provision applies strictly to investigations of fire casualties. It in no way reduces the need for investigators to protect any other PHI to which they have access through other department operations, either deliberately (e.g., EMS call response) or inadvertently (e.g., overheard radio traffic). In particular, because in GCFR’s current structure investigators are also EMTs, they will often function as health care providers, possibly even for a patient from a fire incident they may later investigate. Any PHI obtained by an investigator in his/her role as a health care provider must be protected under the Privacy Rule the same as that of any other patient. The key distinction is in what role the information was obtained.

### ***GCFR Requests for PHI***

If GCFR needs to request PHI from another health care provider on a routine or recurring basis, members shall limit requests to only the reasonably necessary information needed for the intended purpose, as described below. For requests not covered below, members must make this determination individually for each request and they should consult a supervisor or the HIPAA Compliance Officer for guidance. For example, if the request is non-recurring or non-routine, like making a request for documents via a subpoena, GCFR must assure that the request covers only the minimum necessary PHI to accomplish the purpose of the request.

<b>Holder of PHI</b>	<b>Purpose of Request</b>	<b>Information Reasonably Necessary to Accomplish Purpose</b>
Facilities from which patients are transported by GCFR, including assisted living facilities, skilled nursing facilities, doctors’ offices, clinics and urgent care centers, and hospitals	To have pertinent history necessary for adequate patient care during subsequent transport; to have adequate patient records to determine medical necessity for service and to properly bill for services provided.	Transfer sheets, patient face sheets, discharge summaries, Physician Certification Statements and Statements of Medical Necessity, Mobility Assessments
Receiving hospitals	To have adequate patient records to determine medical necessity for service and to properly bill for services provided	Patient face sheets

Other EMS agencies that respond with GCFR	To have adequate patient records to conduct joint treatment and billing operations for patients mutually treated/transported by GCFR	Patient care reports for mutually treated/transported patients
---	--	--

For all other requests, determine what information is reasonably necessary on an individual basis, applying the “minimum necessary” standard in making the determination.

***Incidental Disclosures***

GCFR understands that there will be times when there are incidental disclosures about PHI in the context of caring for a patient. The privacy laws were not intended to impede common health care practices that are essential in providing health care to the individual. Incidental disclosures are inevitable, but these will typically occur in radio or face-to-face conversation between health care providers, or when patient care information in written or computer form is left out in the open for others to access or see.

The fundamental principle is that all members need to be sensitive to the importance of maintaining the confidence and security of all material containing patient information that is created or used. Coworkers and other members should not have access to information that is not necessary for the member to complete his or her job. For example, it is generally not appropriate for field personnel to have access to billing records of the patient.

All personnel must be sensitive to avoiding incidental disclosures to other health care providers and others who do not have a need to know the information. Members should pay attention to who may be listening when they make verbal statements about a patient’s health information, and follow common sense procedures for avoiding accidental or inadvertent disclosures.

***Verbal Security***

Fire Stations and Other Work Areas: Conversation that includes reference to PHI is not permitted except as necessary for members to perform their job tasks related to patient care, billing, supervision, and quality monitoring (as defined above under Role Based Access), and then to the extent that only the minimum necessary information is used to accomplish the intended purpose. ***In particular, casual conversation with one’s coworkers that reveals PHI is not permitted.*** Supervisors are expected to monitor and enforce this provision.

Waiting or Public Areas: If patients are in waiting areas to discuss the service provided to them or to have billing questions answered, make sure that there are no other persons in the waiting area, or if so, bring the patient into a screened or private area before engaging in discussion. In other public areas, members should be sensitive that members of the public and other agencies may be present. Conversations about patients and their health care should not take place in areas where those without a need to know are present.

Other Areas: Members should discuss patient care information only with those who are involved in the care of the patient, regardless of physical location. Members should be sensitive to their

level of voice and to the fact that others may be in the area when appropriate patient-related conversations are taking place. This approach is not meant to impede anyone's ability to speak with other health care providers freely when engaged in the care of the patient. When it comes to treatment of the patient, members should be free to discuss all aspects of the patient's medical condition, treatment provided, and any of the patient's health information members may have in their possession with others involved in the care of the patient, but with the discretion advised above.

Radio Security: Radio transmission for EMS dispatch and response virtually always includes PHI. Members are free to transmit those elements of PHI necessary for effective dispatch and response. To minimize incidental disclosures, members should use discretion and not transmit unnecessary PHI. In particular, radio transmission of patient names and other unique identifiers should be avoided unless absolutely necessary to accomplish necessary treatment or operational tasks.

Members routinely hear radio traffic for responses they are not involved with, much of which contains PHI. ***PHI from such radio traffic shall not be disclosed to anyone.***

### ***Physical Security***

Patient Care Reports and Other Patient or Billing Records: Patient Care Reports (PCRs) shall be stored in a safe and secure manner. When any paper records concerning a patient are completed, they should not be left in open bins or on desktops or other surfaces. Only those with a need to have the information for the completion of their job duties should have access to any paper records.

CADS printouts for EMS calls contain PHI and should not be left in the open. Unless some other legitimate and allowable need exists for printouts, they shall be shredded after completion of the call.

Preliminary documentation (such as handwritten notes) used by a crewmember to assist in the creation or modification of a PCR shall either be submitted to the Fire-Rescue Administration or shredded immediately after completion of the PCR.

In GCFR's computerized patient reporting system, there is normally no need for field personnel to print PCR hard copies, and such printing is discouraged. However, printing is allowed at the discretion of supervisors for legitimate purposes such as reviewing for accuracy and completeness. Any hard copies printed for such purposes shall be immediately shredded after the completion of the task for which it is printed, unless a request otherwise is made by the HIPAA Compliance Officer or the Fire-Rescue Administration. ***Hard copies of PCRs shall not be maintained in station files or in members' possession.***

Billing records, including all notes, remittance advices, charge slips, or claim forms should not be left out in the open and shall be stored securely, with access limited to those who need access to the information for the completion of their job duties.

Offices, fire stations, storage facilities, and other physical facilities containing PHI shall be kept secure to minimize the risk of disclosure to those not authorized to access PHI. Fire station doors shall be kept closed and locked when the station is unoccupied.

### ***Computer Security***

General Computer Security: Station and handheld computers shall be kept secure in such a way to always protect PHI.

Members are permitted to access ONLY their own PCR's unless directed otherwise by department management or the HIPAA Compliance Officer.

E-mail should be regarded as an inherently insecure transmission method. PHI shall not be transmitted by e-mail unless in a password-protected, encrypted, or proprietary file format.

Desktop Computers: Login to the patient reporting software requires a password. Passwords of the user's choosing are issued to EMTs who have been trained on the software. Users needing a new or changed password shall contact an administrator directly to have it assigned. Passwords will not be requested or assigned through other persons. Passwords shall not be disclosed to other users. If a user feels that the security of his/her password has been compromised, he/she shall contact an administrator for a new one. Members shall not log into the patient reporting software under any user name other than their own.

Members should be sensitive to who may be in viewing range of the monitor screen and take simple steps to shield viewing of the screen by unauthorized persons. Members shall not leave EMS Solution software open and unattended on a station PC or a laptop.

CADS Information: In the current GCFR CADS configuration, anyone with CADS access can obtain PHI contained in dispatch records and other CADS files. Therefore, until technological safeguards can better assure role-based access to CADS PHI, procedural safeguards must be maintained. ***Therefore, access to and disclosure of PHI contained in CADS shall be limited to those with a need to know the information based on their role in the organization, and to the minimum necessary information needed for them to perform their job, as described previously.*** Supervisors are expected to monitor this provision to prevent casual browsing and inappropriate access and disclosure of CADS-based PHI.

Remote Devices: The appropriate use of laptop computers, handheld computers, and other remote data entry devices is of utmost concern to GCFR. These devices, collectively referred to as "remote devices," pose a unique and significant patient privacy risk because they may contain confidential patient, staff member, or organizational information. Furthermore, these devices can be easily misplaced, lost, stolen, or accessed by unauthorized individuals. Handheld computers, in particular, pose an even higher risk based on their small size and the fact that, at this time, the patient reporting software installed on them cannot be password protected.

The following practices shall be utilized for remote devices:

1. Remote devices used for capture of PHI will be only those owned and specifically authorized by GCFR.

2. Software will be installed only with the approval of GCFR and in accordance with department and county policies regarding software installation on computers.
3. When unprotected PHI resides on a remote device, the device shall remain in the physical possession of the crew to whom it is assigned. Unprotected PHI includes any open patient records on a device with password protection, and any PHI, open or closed, on a device without password protection.
4. Remote device users shall not permit anyone else, including but not limited to the user's family and/or associates, patients, patient families, or unauthorized staff members, to use GCFR-owned remote devices for any purpose.
5. Upon the loss of a remote device containing any PHI, the GCFR HIPAA Compliance Officer shall be notified immediately.

### **III. Notice of Privacy Practices**

HIPAA requires that in most situations a patient shall be given a Notice of Privacy Practices (NPP), and the provider shall have the patient sign an acknowledgment that he or she received the NPP. HIPAA provides limited exceptions to these NPP requirements for “emergency treatment situations.” It doesn’t define emergency treatment situation, however. The language of the Privacy Rule suggests a much more limited definition of emergency than what we might use. In particular, the Rule clearly is NOT meant to provide blanket exception just because a patient calls 9-1-1. The Rule states:

*“The provisions are intended to provide exceptions for those situations where providing the notice and obtaining an individual’s acknowledgement may not be feasible or practicable. Where such extenuating circumstances do not exist, the Department [of Health and Human Services] expects that covered health care providers are able to provide individuals with a notice and make a good faith effort to obtain their acknowledgement of receipt.”*

Even for true emergencies where it is not “feasible or practicable,” the Rule still requires:

1. An NPP to be delivered as soon after the event as possible, and
2. Documentation as to why a signed acknowledgement was not obtained.

GCFR field providers shall make every reasonable effort to furnish a copy of the NPP to all patients, including those not transported, at the time of treatment or immediately afterward. If because of the patient’s condition or scene circumstances the NPP cannot be handed directly to the patient, other options may be used. Examples include leaving it at the hospital with the patient’s chart (asking the hospital staff to deliver it), or asking a reliable bystander to deliver it at an appropriate time in the future. Such bystander should be one who knows the patient well and seems likely to comply with the request, such as a family member or coworker.

A sufficient supply of NPPs shall be kept on EMS vehicles and in stations.



Members shall obtain, when possible, a signature from the patient that acknowledges receipt of the NPP. Language for this acknowledgement is combined with the language for the assignment of benefits form and signature, and the patient refusal form, so only one signature is necessary for two purposes. If because of the patient's condition or scene circumstances a signature cannot be obtained, the reason for non-signature shall be documented in the PCR.

Each version of the NPP shall be maintained on file for a period of six (6) years after its effective date.

The current GCFR NPP is in the appendix of this Plan.

#### **IV. Medical Records of Employees**

GCFR will, to the extent required by law, protect medical records it receives about employees or other staff in a confidential manner. Generally, only those with a need to know the information will have access to it, and, even then, they will have access only to as much information as is minimally necessary for the legitimate use of the medical records.

In accordance with laws concerning disability discrimination, all medical records of employees will be kept in separate files apart from the employee's general employment file. These records will be secured with limited access by management.

In accordance with the HIPAA Privacy Rule, medical records that are not considered employment records will be treated in accordance with the safeguards of the Privacy Rule with respect to their use and disclosure. Employment records are not considered to be PHI subject to HIPAA safeguards, including certain medical records of employees that are related to the job. These employment records not covered under HIPAA include, but are not limited to: information obtained to determine suitability to perform the job duties (such as physical examination reports), drug and alcohol tests obtained in the course of employment, doctor's excuses provided in accordance with the attendance policy, work-related injury and occupational exposure reports, and medical and laboratory reports related to such injuries or exposures, especially to the extent necessary to determine workers' compensation coverage.

With respect to members of Goochland County Department of Fire-Rescue, health information that is obtained about members in the course of providing ambulance or other medical services directly to them is considered PHI under HIPAA. In other words, if GCFR provides prehospital care to a member, the protections typically given to any patient apply to the member. These protections are subject to limited HIPAA exceptions, such as when the member has suffered a work-related injury or illness while on duty.

As another example, if GCFR receives an employee's medical record in the course of providing the employee with treatment and/or transport, it does not matter that Goochland County Department of Fire-Rescue happens to be the employer – that record is PHI. If, however, the employee submits a doctor's statement to a supervisor to document an absence or tardiness from work, GCFR does not need to treat that statement as PHI. Other health information that could be treated as employment related, and not PHI, includes medical information that is needed for

GCFR to carry out its obligations under the FMLA, ADA, and similar laws, as well as files or records related to occupational injury, disability insurance eligibility, drug screening results, workplace medical surveillance, and fitness-for-duty-tests of employees.

A common practice in the past has been to notify GCFR members, using a mass communications medium such as e-mail, about injuries or illnesses suffered by one of its own. However, when GCFR treats or transports one of its own members, all patient information obtained by the crew that treats or transports the member is considered PHI. Accordingly, all protections afforded to any other form of PHI apply. Except for information described above that is not protected under HIPAA (such as for work-related incidents), all such PHI shall be kept as confidential as any other patient's PHI. Admittedly there may be blurring or even conflict between the role of caregiver (expected to comply with HIPAA) and that of caring coworker (with a well-intentioned desire to notify colleagues about the misfortune of one of their own). But the right of patient privacy, and compliance with the law, shall prevail.

The key issue is the role GCFR is playing in this encounter. To quote from the Privacy Rule:

*“A covered entity must remain cognizant of its dual roles as an employer and as a health care provider. . . . Individually identifiable health information created, received, or maintained by a covered entity in its health care capacity is protected health information. It does not matter if the individual is a member of the covered entity’s workforce or not. . . . When the individual gives his or her medical information to the covered entity as the employer. . . that information becomes part of the employment record, and, as such, is no longer protected health information. . . .”*

*“As explained above, the nature of the information does not determine whether it is an employment record. Rather, it depends on whether the covered entity obtains or creates the information in its capacity as employer or in its capacity as health care provider.”*

## **V. Privacy Training**

All members of Goochland County Department of Fire-Rescue Staff – including all employees, volunteers, students, and trainees (collectively referred to as “members”) who have access to patient information – shall be trained in accordance with the HIPAA Privacy Rule.

All new members will be required to undergo privacy training within a reasonable time upon association with the organization, as scheduled by the HIPAA Compliance Officer. This training shall be delivered before they are allowed to access PHI.

All members will be required to undergo privacy training updates within a reasonable time after there is a material change to County or GCFR policies and procedures on privacy practices.

For purposes of HIPAA, students and interns from external entities are considered part of the GCFR workforce, and shall be considered members under GCFR privacy policies and procedures. They also must meet the same training requirements as employees or volunteers of GCFR. Additionally, their agency or academic institution must have executed a HIPAA Business

Associate Agreement with GCFR before they are allowed access to GCFR PHI. Accordingly, external students and interns shall not be allowed access to PHI until they have completed this training and received clearance from the HIPAA Compliance Officer.

Privacy training will be conducted by the HIPAA Compliance Officer or his or her designee. Attendees will have access to GCFR's policies and procedures regarding privacy. Attendees must attend the training in person and verify attendance and agreement to adhere to GCFR's policies and procedures on privacy practices.

Training will be conducted in a format suitable for the audience, and may include video-based training, live classroom training, computer-aided instruction, or other methods.

Topics of the training will include a complete review of GCFR's Privacy Policy, the GCFR HIPAA Compliance Plan, and other information concerning the HIPAA Privacy Rule, such as, but not limited to the following topic areas:

1. Overview of the federal and state laws concerning patient privacy including the Privacy Regulations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA)
2. Description of protected health information (PHI)
3. Patient rights under the HIPAA Privacy Rule
4. Staff member responsibilities under the Privacy Rule
5. Role of the HIPAA Compliance Officer and reporting employee and patient concerns regarding privacy issues
6. Importance of and benefits of privacy compliance
7. Consequences of failure to follow established privacy policies
8. Use of GCFR's specific privacy forms

## **VI. HIPAA Compliance Officer**

GCFR has appointed a HIPAA Compliance Officer to oversee all activities related to the development, implementation, and maintenance of GCFR's policies and procedures covering the privacy of patient health information. This person serves as the key compliance officer for all federal and state laws that apply to the privacy of patient information, including the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The HIPAA Compliance Officer is also available to members for consultation on any issues or concerns they have about how GCFR deals with protected health information. Members should feel free to contact the HIPAA Compliance Officer at any time with questions or concerns. GCFR will not retaliate against any staff member who expresses a legitimate concern or complaint about any policy or practice related to the safeguarding of patient information and GCFR's legal obligations to protect patient privacy.

The HIPAA Compliance Officer is tasked with the responsibility of ensuring that all of the organization's patient information privacy policies and procedures related to the privacy of, and access to, patient health information are followed.

### ***HIPAA Compliance Officer – Principle Responsibilities***

1. Serves as a resource for all members for any question or issue related to HIPAA and patient privacy.
2. Develops policies and procedures on staff training related to the privacy of patient health information and protected health information.
3. Develops policies on the security of health care information including computer and password security and patient data integrity.
4. Defines levels of staff access to PHI and minimum necessary requirement for staff based on the required job responsibilities.
5. Oversees, directs, delivers, and ensures the delivery of initial and ongoing privacy training and orientation to all staff members, employees, volunteers, students and trainees.
6. Serves as the contact person for the dissemination of PHI to other health care providers.
7. Serves as the contact person for patient complaints and requests.
8. Processes patient requests for access to and amendment of health information and consent forms.
9. Processes all patient accounting requests.
10. Ensures the capture and storage of patient PHI for the minimum period required by law.
11. Ensures GCFR compliance with all applicable Privacy Rule requirements and works with management and the County Attorney to ensure that GCFR maintains appropriate privacy and confidentiality notices and forms and materials.
12. Works with state and federal government agencies charged with compliance reviews, audits, and investigations.
13. Performs regular evaluations to assure that technical and non-technical safeguards and current practices meet current HIPAA regulations.

## **VII. Patient Requests for Protected Health Information**

Under the HIPAA Privacy Rule, individuals have the right to access and to request amendment or restriction on the use of their PHI maintained in the Designated Record Set (DRS). (See section VIII, “Designated Record Sets”).

To ensure that patient rights are assured, this section outlines procedures for requests for patient access, amendment, and restriction on the use of PHI. It also describes the disclosure accounting process GCFR will use.

Only information contained in the DRS outlined in this Plan is to be provided to patients who request access, amendment, or restriction on the use of their PHI in accordance with the Privacy Rule and GCFR policies and procedures.

Patients have the right to complain to GCFR about any concerns they may have concerning patient privacy. The HIPAA Compliance Officer is responsible for receiving, investigating, and documenting all complaints concerning patient privacy issues.

All persons requesting access to, amendment to, or restriction on use of PHI, or wish to lodge a complaint on the handling of their PHI, shall be referred to the Fire-Rescue Administration.

Where “patient” is referred to in this procedure, it also includes a patient’s authorized legal representative, such as a parent or guardian.

### ***Procedure for Patient or Authorized Representative Access***

1. Upon presentation to the Fire-Rescue Administration office, the patient or appropriate representative will complete a Request for Access Form.
2. The GCFR member shall verify the requestor’s identity. The use of a driver’s license, social security card, or other form of government-issued identification is acceptable for this purpose. If the requestor is someone other than the patient, the GCFR employee shall verify the name of the individual, the reason for the request, and that the member has a legal right to access PHI.
3. The completed form will be presented to the GCFR HIPAA Compliance Officer for action.
4. The GCFR HIPAA Compliance Officer will act upon the request within 30 days, preferably sooner. Generally, GCFR must respond to requests for access to PHI within 30 days of receipt of the access request, unless the designated record set is not maintained on site, in which case the response period may be extended to 60 days.
5. If GCFR is unable to respond to the request within these time frames, the requestor must be given a written notice no later than the initial due date for a response, explaining why

GCFR could not respond within the time frame, in which case GCFR may extend the response time by an additional 30 days.

6. Upon approval of access, the patient will have the right to access the PHI contained in the DRS outlined in Section VIII of this Plan. Once access is approved, they may also request a copy of the PHI contained in the DRS upon verbal or written request.
7. Patient access may be denied for the reasons listed below, and in some cases the denial of access may be appealed to GCFR for review.
8. The following are reasons to deny access to PHI that are not subject to review, are final, and may not be appealed by the patient:
  - a. If the requested information was compiled in reasonable anticipation of, or use in, a civil, criminal or administrative action or proceeding;
  - b. If the requested information was obtained from someone other than a health care provider under a promise of confidentiality and the access would be reasonably likely to reveal the source of the information.
9. The following reasons to deny access to PHI are subject to review and the patient or representative may appeal the denial. The decision to deny access using one or more of these criteria will be made by the GCFR Operational Medical Director (OMD).
  - a. If the OMD has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;
  - b. If the PHI makes reference to another person (other than a health care provider) and the OMD has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to that person;
  - c. If the request for access is made by a requestor as a personal representative of the individual about whom the requestor is requesting the information, and the OMD has determined, in the exercise of professional judgment, that access by the requestor is reasonably likely to cause harm to the individual or another person.
  - d. If the denial of the request for access to PHI is for reasons a, b, or c, then the patient may request a review of the denial of access by sending a written request to the HIPAA Compliance Officer.
  - e. GCFR will designate a licensed health professional, who was not directly involved in the denial, to review the decision to deny the patient access. The GCFR HIPAA Compliance Officer will promptly refer the request to this designated review official. The review official will determine within a reasonable period of time whether the denial is appropriate. GCFR will provide the patient with written notice of the determination of the designated reviewing official.

- f. The patient may also file a complaint in accordance with the Procedure for Filing Complaints about Privacy Practices if the patient is not satisfied with GCFR's determination.
10. Access to the actual files or computers that contain the DRS that may be accessed by the patient or requestor shall not be permitted. Rather, PCR printouts or copies of the records should be provided for the patient or requestor to view in a confidential area under the direct supervision of a designated GCFR staff member. ***Under no circumstances shall originals of PHI leave the premises.***
11. If the patient or requestor would like to retain copies of the DRS provided, then GCFR may charge a reasonable fee for the costs of reproduction.
12. Whenever a patient or requestor accesses PHI from the DRS, a notation shall be maintained in a log book or data base indicating the time and date of the request, the date access was provided, what specific records were provided for review, and what copies were left with the patient or requestor.
13. Following a request for access to PHI, a patient or requestor may request an amendment to his or her PHI, and request restriction on its use in some circumstances.

#### ***Requests for Amendment to PHI***

14. The patient or appropriate requestor may request amendment only to PHI contained in the DRS. The "Request for Amendment of PHI" Form must accompany any request for amendment.
15. GCFR must act upon a Request for Amendment within 60 days of the request. If GCFR is unable to act upon the request within 60 days, it must provide the requestor with a written statement of the reasons for the delay, and in that case may extend the time period in which to comply by an additional 30 days.
16. All requests for amendment shall be forwarded immediately to the HIPAA Compliance Officer for review.

#### **Granting Requests for Amendment**

17. If the HIPAA Compliance Officer grants the request for amendment, then the requestor will receive a letter indicating that the appropriate amendment to the PHI or record that was the subject of the request has been made.
18. There must be written permission provided by the patient so that that GCFR may notify the persons with which the amendments need to be shared. GCFR must provide the amended information to those individuals identified by having received the PHI that has been amended as well as those persons or business associates that have such information and who may have relied on or could be reasonably expected to rely on the amended PHI.

19. The patient must identify individuals who may need the amended PHI and sign the statement in the Request for Amendment form giving GCFR permission to provide them with the updated PHI.
20. GCFR will add the request for amendment, the denial or granting of the request, as well as any statement of disagreement by the patient and any rebuttal statement by GCFR to the designated record set.

#### Denial of Requests for Amendment

21. GCFR may deny a request to amend PHI for the following reasons:
  - a. If GCFR did not create the PHI at issue,
  - b. If the information is not part of the DRS, or
  - c. The information is accurate and complete.
22. GCFR must provide a written denial, and the denial must be written in plain language and state the reason for the denial; the individual's right to submit a statement disagreeing with the denial and how the individual may file such a statement; a statement that, if the individual does not submit a statement of disagreement, the individual may request that the provider provide the request for amendment and the denial with any future disclosures of the PHI; and a description of how the individual may file a complaint with the covered entity, including the name and telephone number of an appropriate contact person, or to the Secretary of Health and Human Services.
23. If the individual submits a "statement of disagreement," the provider may prepare a written rebuttal statement to the patient's statement of disagreement. The statement of disagreement will be appended to the PHI, or at GCFR's option, a summary of the disagreement will be appended, along with the rebuttal statement of GCFR.
24. If GCFR receives a notice from another covered entity, such as a hospital, that it has amended its own PHI in relation to a particular patient, the ambulance service must amend its own PHI that may be affected by the amendments.

#### ***Requests for Restriction***

25. The patient may request a restriction on the use and disclosure of their PHI.
26. GCFR is not required to agree to any restriction, and given the emergent nature of our operation, we generally will not agree to a restriction.
27. ALL REQUESTS FOR RESTRICTION ON USE AND DISCLOSURE OF PHI MUST BE SUBMITTED IN WRITING ON THE APPROVED GCFR FORM. ALL REQUESTS WILL BE REVIEWED AND DENIED OR APPROVED BY THE HIPAA COMPLIANCE OFFICER.



28. If GCFR agrees to a restriction, it may not use or disclose PHI in violation of the agreed upon restriction, except that if the individual who requested the restriction is in need of emergency service, and the restricted PHI is needed to provide the emergency service, GCFR may use the restricted PHI or may disclose such PHI to another health care provider to provide treatment to the individual.
29. The agreement to restrict PHI will be documented to ensure that the restriction is followed.
30. A restriction may be terminated if the individual agrees to or requests the termination. Oral agreements to terminate restrictions must be documented. A current restriction may also be terminated by GCFR as long as GCFR notifies the patient that PHI created or received after the restriction is removed is no longer restricted. PHI that was restricted prior to GCFR voiding the restriction must continue to be treated as restricted PHI.

### ***Accounting for Uses and Disclosures of PHI***

31. All patient records will be kept by GCFR for a period of at least six (6) years from date of service.
32. All patient accounting requests should be received directly from a patient or authorized representative.
33. GCFR will provide a list of uses and disclosures of the patient's PHI, made by GCFR or a business associate on GCFR's behalf, for the last six (6) years, or to the extent that GCFR has been required to maintain that patient's information if less than six (6) years.
34. All uses and disclosures of a patient's PHI, made by GCFR, must be documented for accounting purposes except:
  - a. Disclosures to carry out treatment, payment, and health care operations,
  - b. Disclosures to the patient or authorized representative of the patient's own PHI,
  - c. For national security or intelligence purposes,
  - d. For which GCFR has received authorization from the patient or authorized representative,
  - e. Uses and disclosures incident to an unaccountable use or disclosure,
  - f. That occurred prior to the compliance date,
  - g. To correctional institutions and staff as provided for in the Privacy Rule,
  - h. As part of a limited data set as provided for in the Privacy Rule, such as the data set submitted to the Virginia Office of EMS as required by state law.
35. A common use or disclosure that must be accounted for and information provided upon a request for accounting is the disclosure of PHI in response to a subpoena, summons, or warrant.

## VIII. Designated Record Sets

To ensure that Goochland County Department of Fire-Rescue releases Protected Health Information (PHI) in accordance with the Privacy Rule, this section defines information that should be accessible to patients as part of the Designated Record Set (DRS) and outlines procedures for requests for patient access, amendment, and restriction on the use of PHI.

Under the Privacy Rule, the DRS includes medical and billing records that are created or used by GCFR to make decisions about the patient. The DRS should include only PHI covered by HIPAA, and should not include information used for the operational purposes of the organization, such as quality management data, accident reports, and incident reports. It should also not include employment related health information not covered by HIPAA, such as worker's compensation claim information.

The DRS for any requests for access to PHI includes the following records:

1. The patient care report (PCR) and related documents created by EMS field personnel. This includes any photographs, monitor strips, Physician Certification Statements, Refusal of Care forms, or other source data that is incorporated into, submitted with, and/or attached to the PCR.
2. The electronic claims records or other paper records of submission of actual claims to Medicare or other insurance companies.
3. Any patient-specific claim information, including responses from insurance payers, such as remittance advice statements, Explanation of Medicare Benefits (EOMBs), charge screens, patient account statements, and signature authorization and agreement to pay documents.
4. Medicare Advance Beneficiary Notices, notices from insurance companies indicating coverage determinations, documentation submitted by the patient, and copies of the patient's insurance card or policy coverage summary, that relate directly to the care of the patient.
5. Amendments to PHI, or statements of disagreement by the patient requesting the amendment when PHI is not amended upon request, or an accurate summary of the statement of disagreement.

The DRS also include copies of records created and provided to GCFR by other service providers and other health care providers such as other EMS agencies, air medical services, nursing homes, hospitals, police departments, medical examiner's office, etc., that are used by GCFR as part of treatment and payment purposes related to the patient.

## **IX. Complaints and Privacy Breaches**

GCFR shall make all reasonable efforts to investigate and mitigate the effects of complaints and potential breaches of privacy.

All reports of complaints and potential privacy breaches shall be referred to the HIPAA Compliance Officer. If an investigation is required, the HIPAA Compliance Officer will forward pertinent details to the appropriate GCFR manager (typically an Executive Chief Officers) for investigation. The HIPAA Compliance Officer will provide consultation to the manager as needed to assist in the investigation. The manager will provide a written report to the HIPAA Compliance Officer upon completion of the investigation, including whether a violation of the GCFR HIPAA policy or Compliance Plan has occurred.

The HIPAA Compliance Officer will maintain a record of all reported complaints and potential privacy breaches, including investigation reports, disposition of issues, and mitigation steps taken. The HIPAA Compliance Officer will regularly review these records to determine and recommend whether system improvements are needed to reduce the risk of a reoccurrence and assure compliance with the current regulation. Such improvements may include, but are not limited to:

- Training
- Policy or Compliance Plan updates
- Modification of methods of safeguarding PHI
- Physical or technological enhancements

Those wishing to file a complaint may use the “Procedure for Filing Complaints about Privacy Practices,” a copy of which is contained in the appendix of this plan.

All complaints and reports of potential privacy breaches shall be kept confidential. Those who make such complaints or reports will not be retaliated against in any way.

## **X. Appendix – Forms**

**Goochland County Department of Fire-Rescue  
Notice of Privacy Practices**

**THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE  
USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS  
INFORMATION. PLEASE REVIEW IT CAREFULLY.**

Goochland County Department of Fire-Rescue (“GCFR”) is required by law to maintain the privacy of certain confidential health care information, known as Protected Health Information or PHI, and to provide you with a notice of our legal duties and privacy practices with respect to your PHI. GCFR is also required to abide by the terms of the version of this Notice currently in effect.

*Uses and Disclosures of PHI:* GCFR may use PHI for the purposes of treatment, payment, and health care operations, in most cases without your written permission. Examples of our use of your PHI:

For treatment. This includes such things as obtaining verbal and written information about your medical condition and treatment from you as well as from others, such as doctors and nurses who give orders to allow us to provide treatment to you. We may give your PHI to other health care providers involved in your treatment, and may transfer your PHI via radio or telephone to the hospital or dispatch center.

For payment. This includes any activities we must undertake in order to get reimbursed for the services we provide to you, including such things as submitting bills to insurance companies, making medical necessity determinations, and collecting outstanding accounts.

For health care operations. This includes quality assurance activities, licensing, and training programs to ensure that our personnel meet our standards of care and follow established policies and procedures, as well as certain other management functions.

Reminders for Scheduled Transports and Information on Other Services. We may also contact you to provide you with a reminder of any scheduled appointments for non-emergency ambulance and medical transportation, or to provide information about other services we render.

Fundraising. We may contact you when we are in the process of raising funds for Goochland County Department of Fire-Rescue, or to provide you with information about our annual subscription program called EMS Passport.

*Use and Disclosure of PHI Without Your Authorization.* GCFR is permitted to use PHI *without* your written authorization, or opportunity to object, in certain situations, and unless prohibited by a more stringent state law, including:

- For the treatment, payment, or health care operations activities of another health care provider who treats you;
- As required by law, including reporting for public health purposes;
- To a family member, other relative, or close personal friend or other individual involved in your care if we obtain your verbal agreement to do so or if we give you an opportunity

to object to such a disclosure and you do not raise an objection, and in certain other circumstances where we are unable to obtain your agreement and believe the disclosure is in your best interests;

- To report abuse, neglect or domestic violence;
- For health oversight activities including audits or government investigations, inspections, disciplinary proceedings, and other administrative or judicial actions undertaken by the government (or their contractors) by law to oversee the health care system;
- For judicial and administrative proceedings as required by a court or administrative order, or in some cases in response to a subpoena, discovery request, or other legal process;
- For law enforcement activities in limited situations, such as when responding to a warrant;
- For military, national defense and security, and other special government functions;
- To avert a serious threat to the health and safety of a person or the public at large;
- For workers' compensation purposes, and in compliance with workers' compensation laws;
- To coroners, medical examiners, and funeral directors for identifying a deceased person, determining cause of death, or carrying on their duties as authorized by law;
- If you are an organ donor, we may release health information to organizations that handle organ procurement or organ, eye or tissue transplantation or to an organ donation bank, as necessary to facilitate organ donation and transplantation;
- For research projects, but this will be subject to strict oversight and approvals;
- We may also use or disclose health information about you in a way that does not personally identify you or reveal who you are.

Any other use or disclosure of PHI, other than those listed above will be made only with your written authorization. You may revoke your authorization at any time, in writing, except to the extent that we have already used or disclosed medical information in reliance on that authorization.

*Patient Rights:* As a patient, you have a number of rights with respect to your PHI, including:

*The right to access, copy, or inspect your PHI.* This means you may inspect and copy most of the medical information about you that we maintain. We will normally provide you with access to this information within 30 days of your request. We may also charge you a reasonable fee for you to copy any medical information that you have the right to access. In limited circumstances, we may deny you access to your medical information, and if you disagree with our decision, you may obtain a review of certain types of denials. We have available forms to request access to your PHI. We will provide a written response if we deny you access and let you know your review rights. You also have the right to receive confidential communications of your PHI. To assure your records are discussed and disclosed only to the proper person (you or your legally authorized representative), we normally require you to appear in person at our office to access or discuss your medical information. However, we will honor reasonable requests by you to receive communications about your medical information by alternative means or at alternative locations. If you wish to inspect and copy your medical information, you should contact our HIPAA Compliance Officer, whose address and phone number are listed below.

*The right to amend your PHI.* You have the right to ask us to amend written medical information that we may have about you if you think it is inaccurate or incomplete. We will generally amend your information within 60 days of your request and will notify you when we have amended the information. We are permitted by law to deny your request to amend your medical information only in certain circumstances, like when we believe the information you have asked us to amend is correct and complete. If you wish to request that we amend the medical information that we have about you, you should contact our HIPAA Compliance Officer.

*The right to request an accounting.* We are required to keep a record of certain disclosures of your medical information, and you may request an accounting of what that record contains. Disclosures that we are NOT required to keep a record of include:

- Information we have used or disclosed for purposes of treatment, payment or health care operations,
- When we share your health information with our business associates, like our billing company or a medical facility from or to which we have transported you, or
- Information for which you have already given us written authorization to disclose.

We are required to keep this record of disclosures for the past six years, or back to the compliance date of January 1, 2013 for federal privacy regulations, whichever is later. If you wish to request an accounting of these disclosures, contact our HIPAA Compliance Officer.

*The right to request that we restrict the uses and disclosures of your PHI.* You have the right to request that we restrict how we use and disclose the medical information that we have about you. GCFR is not required to agree to any restrictions you request, but any restrictions agreed to by GCFR in writing are binding on GCFR.

*Internet, Electronic Mail, and the Right to Obtain Copy of Paper Notice on Request.* If we maintain a web site, we will prominently post a copy of this Notice on our web site. If you allow us, we will forward you this Notice by electronic mail instead of on paper and you may always request a paper copy of the Notice.

*Revisions to the Notice:* GCFR reserves the right to change the terms of this Notice at any time, and the changes will be effective immediately and will apply to all protected health information that we maintain. Any material changes to the Notice will be promptly posted in our facilities and posted to our web site, if we maintain one. You can get a copy of the latest version of this Notice by contacting our HIPAA Compliance Officer.

*Your Legal Rights and Complaints:* You also have the right to complain to us, or to the Secretary of the United States Department of Health and Human Services if you believe your privacy rights have been violated. You will not be retaliated against in any way for filing a complaint with us or to the government. Should you have any questions, comments, or complaints you may direct all inquiries to our HIPAA Compliance Officer.

*HIPAA Compliance Officer Contact Information:*

HIPAA Compliance Officer  
Goochland County Department of Fire-Rescue  
PO Box 247  
Goochland, Virginia 23063  
(804) 556-5344

*Effective Date of the Notice:* January 1, 2013

*Revisions:* June 13, 2016  
March 13, 2023



**Goochland County Department of Fire-Rescue  
Patient Request for Access Form**

Patient Name: \_\_\_\_\_ Date: \_\_\_\_\_

Address: \_\_\_\_\_

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip Code: \_\_\_\_\_

Social Security No.: \_\_\_\_\_

Last Date of Service: \_\_\_\_\_

*Patient Rights:* As a patient, you have the right to access, copy or inspect your protected health information, or PHI, in accordance with federal law. You may also have the right to request an amendment to your PHI, or request that we restrict the use and disclosure of it. These rights are further described in our Notice of Privacy Practices and in other policies which you may have upon request.

To better allow us to process your request, please indicate the type of request you are making on this form: [check all that apply]

\_\_\_\_\_ Access to simply review my health information.

\_\_\_\_\_ Access to obtain copies of my health information.

\_\_\_\_\_ Access to review and potentially request amendment of my health information.

\_\_\_\_\_ Access to review and potentially request an accounting of how my PHI has been used and disclosed to others.

\_\_\_\_\_ Access to review and potentially request restrictions on the use and disclosure of my health information.

*Signature* \_\_\_\_\_ *Request Date* \_\_\_\_\_

**Goochland County Department of Fire-Rescue  
Denial of Request for Access to Protected Health Information**

Dear [INSERT REQUESTOR'S NAME]:

We have carefully reviewed your request to have access to certain protected health information (PHI) that Goochland County Department of Fire-Rescue has in its possession about you. Unfortunately, we are unable to grant your request for access to this information.

The basis for this denial is that:

1. \_\_\_\_ The information you requested was compiled in reasonable anticipation of, or use in, a civil, criminal or administrative action or proceeding;
2. \_\_\_\_ The information you requested was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

The denials for reasons #1 or #2 are final and you may not appeal the decision to deny access to the information.

3. \_\_\_\_ Our operational medical director (OMD) has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;
4. \_\_\_\_ The protected health information makes reference to another person (other than a health care provider) and our OMD has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to that person;
5. \_\_\_\_ The request for access is made by you as a personal representative of the individual about whom you are requesting the information, and our OMD has determined, in the exercise of professional judgment, that access by you is reasonably likely to cause harm to the individual or another person.

Denials of access for reasons #3, #4, or #5 may be reviewed in accordance with the review procedures described below.

Review Procedures

If the denial of your request for access to PHI is for reasons #3, 4 or 5, you may request a review of the denial of access by sending a written request to:

HIPAA Compliance Officer  
Goochland County Fire-Rescue  
PO Box 247  
Goochland, VA 23063

We will designate a licensed health professional, who was not directly involved in the denial, to review the decision to deny you access. We will promptly refer your request to this designated review official. The review official will determine within a reasonable period of time whether the denial is appropriate. We will provide you with written notice of the determination of the designated review official.

You may also file a complaint in accordance with our enclosed complaint procedures (available upon request) if you are not satisfied with our determination.

Sincerely,

HIPAA Compliance Officer  
Gochland County Department of Fire-Rescue

**Goochland County Department of Fire-Rescue  
Request for Amendment of Protected Health Information**

Patient Name: \_\_\_\_\_

Address: \_\_\_\_\_

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip Code: \_\_\_\_\_

**Information to Amend:**

Please check the field that represents the type of information you would like to amend.

- |  |   |
|--|---|
| <input type="checkbox"/> Name                      | <input type="checkbox"/> Marital Status           |
| <input type="checkbox"/> Billing Address           | <input type="checkbox"/> Surrogate Decision Maker |
| <input type="checkbox"/> Mailing Address           | <input type="checkbox"/> Organ Donor              |
| <input type="checkbox"/> Current Medical Condition | <input type="checkbox"/> Other: Please describe   |
| <input type="checkbox"/> Past Medical History      | _____   |
| <input type="checkbox"/> Current Medications       | _____   |
| <input type="checkbox"/> Allergies                 | _____   |

Please specifically describe what information you wanted amended. Please list ONLY the new information. Attach a separate sheet if necessary.

---

---

---

---

---

---

---

---

---

---

Goochland County Department of Fire-Rescue, in its capacity as a health care provider, is entitled to perform and bill for services based on all protected health information in its current form or upon which it has already relied until such time as the amended information becomes effective. Goochland County Department of Fire-Rescue is not required to accept your request for amendment and will notify you in writing as to the decision on your request.

Your signature below indicates that you have agreed to accept these terms as they have been listed and to provide payment, if required, to Goochland County Department of Fire-Rescue based on existing protected information until such time that the amendments you have made are effective.

*Patient Signature:* \_\_\_\_\_ *Date:* \_\_\_\_\_

**Goochland County Department of Fire-Rescue  
Acceptance of Request for Amendment of Protected Health Information**

Dear [INSERT NAME OF REQUESTOR]:

We have reviewed your request for amendment to the protected health information (PHI) of [INSERT NAME OF PATIENT]. Please be advised that we have made the appropriate amendment to the PHI or record that was the subject of your request.

We are now requesting that you grant us permission to allow us to notify the persons with which the amendments need to be shared. We will provide to those individuals you identify to us as having received the PHI that has been amended as well as those persons or business associates that have such information and who may have relied on or could be reasonably expected to rely on the amended PHI.

Identify to us any individuals you know of who may need the amended PHI about you and sign the statement below giving us permission to provide them with the updated PHI.

If you have any questions, please contact the GCFR HIPAA Compliance Officer, Goochland County Department of Fire-Rescue, PO Box 247, Goochland, Virginia, 23063, (804) 556-5304.

Sincerely,

Goochland County Department of Fire-Rescue

By my signature below, I hereby agree to allow Goochland County Department of Fire-Rescue to provide amended PHI that it may have about me to the following persons, and to others who Goochland County Department of Fire-Rescue has identified have a need for such information, provided such information is furnished in accordance with federal law.

Contact information for persons I know need the amended PHI about me:

---

---

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature

**Gochland County Department of Fire-Rescue**  
**Denial of Request for Amendment to Protected Health Information**

Dear [INSERT NAME OF REQUESTOR]:

We have reviewed your request for amendment to the protected health information (PHI) of [INSERT NAME OF PATIENT]. Please be advised that we must deny your request to amend this information at this time.

The basis for this denial is:

[NOTE: YOU MUST GIVE A PLAIN LANGUAGE REASON FOR THE DENIAL. YOU MAY DENY THE REQUEST FOR AMENDMENT IF: 1) YOU DID NOT CREATE THE PHI AT ISSUE, 2) THE INFORMATION IS NOT PART OF A DESIGNATED RECORD SET, OR 3) THE INFORMATION IS ACCURATE AND COMPLETE]

You have the right to submit a written statement to us if you disagree with our denial of your request. You may file your statement directly to our HIPAA Compliance Officer, [INSERT NAME] at the address listed above.

If you do not submit a statement disagreeing with our decision to deny your amendment request, you may request that we provide your initial request for amendment, and a copy of our denial of your request with any future disclosures of the protected health information (PHI) that was the subject of your request for denial.

You also have the right to file a complaint with us or with the federal government if you disagree with our decision to deny your request to amend your PHI. We have enclosed a copy of our Complaint Procedure, which outlines the steps you need to take to file either a complaint with us, or a complaint with the federal government.

Sincerely,

HIPAA Compliance Officer  
Gochland County Department of Fire-Rescue

**Goochland County Department of Fire-Rescue  
Patient Accounting Form**

Patient Name: \_\_\_\_\_ Date: \_\_\_\_\_

Address: \_\_\_\_\_

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip Code: \_\_\_\_\_

Social Security No.: \_\_\_\_\_

*Patient Rights:* As a patient, you have the right to access, copy or inspect your PHI, amend your PHI, request an accounting of certain uses and disclosures of PHI for the last six (6) years (or since the compliance date of 4/14/03 of federal privacy regulations, whichever is later), prior to the date of the request, from Goochland County Department of Fire-Rescue. **NOTE: Goochland County Department of Fire-Rescue is not required to provide you with an accounting of uses and disclosures associated with your treatment and transport, or for billing, payment, or health care operations.**

*Signature* \_\_\_\_\_ *Request Date* \_\_\_\_\_

**List of Uses and Disclosures**

Date of Disclosure	Name/Address of Recipient	Purpose and Brief Description of Disclosure	PHI Disclosed

**GOOCHLAND COUNTY DEPARTMENT OF FIRE-RESCUE**  
**Accounting Log for Disclosures of Protected Health Information**

DATE OF DISCLOSURE	PATIENT NAME	REQUESTOR NAME/COMPANY/TITLE	PURPOSE OF DISCLOSURE	PHI REQUESTED (DESCRIBE)	AUTHORIZATION FROM PATIENT?	PHI DISCLOSED (DESCRIBE)	PRIVACY OFFICER REVIEW



**Goochland County Department of Fire-Rescue  
Patient Request for Restriction Form**

Patient Name: \_\_\_\_\_ Date: \_\_\_\_\_

Address: \_\_\_\_\_

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip Code: \_\_\_\_\_

Social Security No.: \_\_\_\_\_

*Patient Rights:* As a patient, you have the right to request restrictions to the uses and disclosures of your PHI. **Goochland County Department of Fire-Rescue is not required to agree to any restrictions requested by the patient, however any restrictions agreed to by Goochland County Department of Fire-Rescue are binding on Goochland County Department of Fire-Rescue.**

Please indicate your request for restricted uses and disclosures of your PHI.

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Signature \_\_\_\_\_ Date \_\_\_\_\_

-----  
**FOR GCFR USE ONLY**

**DATE RECEIVED** \_\_\_\_\_

**REQUEST ACCEPTED** \_\_\_\_\_

**REQUEST DENIED** \_\_\_\_\_

**DATE** \_\_\_\_\_

**REVIEWING OFFICIAL** \_\_\_\_\_

**NOTICE TO PT** \_\_\_\_\_

**COMMENTS:**

\_\_\_\_\_  
\_\_\_\_\_

**Goochland County Department of Fire-Rescue  
Authorization to Use and Disclose  
Specific Protected Health Information**

By signing this Authorization, I hereby direct the use or disclosure by Goochland County Department of Fire-Rescue of certain medical information pertaining to my health, my health care, or me.

This Authorization concerns the following medical information about me:

---

---

---

This information may be used or disclosed by Goochland County Department of Fire-Rescue and may be disclosed to:

---

[LIST NAME OR SPECIFIC IDENTIFICATION OF THE PERSON(S) OR CLASS OF PERSONS TO WHOM YOU MAY MAKE THE REQUESTED USE/DISCLOSURE]

I understand that I have the right to revoke this Authorization at any time except to the extent that Goochland County Department of Fire-Rescue has already acted in reliance on the Authorization. To revoke this Authorization, I understand that I must do so by written request to:

HIPAA Compliance Officer  
Goochland County Department of Fire-Rescue  
PO Box 247  
Goochland, Virginia 23063  
(804) 556-5304

I understand that information used or disclosed pursuant to this Authorization may be subject to redisclosure by the recipient and no longer subject to privacy protections provided by law.

I understand that my written authorization is not required for Goochland County Department of Fire-Rescue to use my protected health information for treatment, payment, and health care operations.

I understand that I have the right to inspect and copy the information that is to be used or disclosed as part of this Authorization. The Authorization is being requested by Goochland County Department of Fire-Rescue for the following purpose(s):

---

---

---

The use or disclosure of the requested information will \_\_\_/will not \_\_\_ result in direct or indirect remuneration to Goochland County Department of Fire-Rescue from a third party.

I acknowledge that I have read the provisions in the Authorization and that I have the right to refuse to sign this Authorization. I understand and agree to its terms.

\_\_\_\_\_ [Name] \_\_\_\_\_ [Date]

\_\_\_\_\_ [Description of the authority of personal representative, if applicable]

**Goochland County Department of Fire-Rescue  
Procedure for Filing Complaints about Privacy Practices**

**YOU MAY MAKE A COMPLAINT DIRECTLY TO US**

You have the right to make a complaint directly to the HIPAA Compliance Officer of Goochland County Department of Fire-Rescue concerning our policies and procedures with respect to the use and disclosure of protected health information (PHI) about you. You may also make a complaint about concerns you have regarding our compliance with any of our established policies and procedures concerning the confidentiality and use or disclosure of your PHI, or about the requirements of the federal Privacy Rule.

All complaints should be directed to our HIPAA Compliance Officer at the following address and phone number:

HIPAA Compliance Officer  
Goochland County Department of Fire-Rescue  
PO Box 247  
Goochland, Virginia 23063  
(804) 556-5344

If you are dissatisfied with our response to a complaint, you may contact the Goochland County Attorney at the following address and phone number:

Goochland County Attorney's Office  
PO Box 10  
1800 Sandy Hook Road  
Goochland, Virginia 23063  
(804) 556-5877

**YOU MAY ALSO MAKE A COMPLAINT TO THE GOVERNMENT**

If you believe Goochland County Department of Fire-Rescue is not complying with the applicable requirements of the Federal Privacy Rule you may file a complaint with the U.S. Department of Health and Human Services Office of Civil Rights (OCR). The OCR may investigate complaints. Such investigation may include a review of the pertinent policies, procedures, or practices of the covered entity and of the circumstances regarding any alleged acts or omissions concerning compliance.

Complaints to the OCR should be submitted to:

OCR Regional Manager  
Office for Civil Rights  
U.S. Department of Health and Human Services  
150 S. Independence Mall West – Suite 372  
Philadelphia, PA 19106-3499  
(215) 861-4441  
(215) 861-4440 (TDD)  
(215) 861-4431 (Fax)  
E-mail: [OCRComplaint@hhs.gov](mailto:OCRComplaint@hhs.gov)

The Privacy Rule states the following:

*Requirements for filing complaints.* Complaints under this section must meet the following requirements:

(1) A complaint must be filed in writing, either on paper or electronically. OCR recommends that you use the OCR Health Information Privacy Complaint Form, which can be found on its Web site or at an OCR Regional Office. The OCR Web site is:

<http://www.hhs.gov/ocr/hipaa>

(2) A complaint must name the entity that is the subject of the complaint and describe the acts or omissions believed to be in violation of the applicable requirements of the Federal Privacy Rule or the applicable standards, requirements, and implementation specifications of subpart E of part 164 of the Federal Privacy Rule.

(3) A complaint must be filed within 180 days of when the complainant knew or should have known that the act or omission complained of occurred. The OCR may extend the 180-day period if good cause can be shown. Any alleged violation must have occurred on or after January 1, 2013 for the OCR to have the authority to investigate.

The Secretary may prescribe additional procedures for the filing of complaints, as well as the place and manner of filing, by notice in the Federal Register.

**Goochland County Department of Fire-Rescue**  
**Log for Processing Complaints about Privacy Practices**

<b>DATE COMPLAINT RECEIVED</b>	<b>PATIENT NAME</b>	<b>DESCRIPTION OF COMPLAINT</b>	<b>DISPOSITION OF COMPLAINT</b>

**Goochland County Department of Fire-Rescue  
Privacy Training Record Form**

Topic: "HIPAA Awareness and the Protection of Patient Privacy"

Date of Training: \_\_\_\_\_

Time Training Began: \_\_\_\_\_

Time Training Ended: \_\_\_\_\_

**IMPORTANT! SIGN IN AND VERIFICATION REQUIRED\***

By my signature below, I verify that I have attended the training session described above and that I will adhere to the Goochland County Department of Fire-Rescue HIPAA Policy and Compliance Plan, a copy of which I have had the opportunity to review before or during this session.

Date	Name (Please Print)	Signature Verification of Attendance

**Goochland County Department of Fire-Rescue  
List of Designated Privacy Officials**

The following is a list of individuals who are responsible for various aspects of Federal Privacy Rule. When in doubt, you should contact the designated HIPAA Compliance Officer, who oversees the Department's privacy compliance issues:

**HIPAA COMPLIANCE OFFICER:** This person may be contacted with questions about requests to access, amend, or limit disclosure of protected health information (PHI), request an accounting of certain PHI disclosures, and to register a complaint about patient privacy issues.

HIPAA Compliance Officer  
Goochland County Department of Fire-Rescue  
PO Box 247  
Goochland, Virginia 23063  
(804) 556-5344

**OTHER CONTACTS FOR COMPLAINTS:** In the event that the GCFR HIPAA Compliance Officer has not satisfactorily resolved the issue, those wishing to register a complaint about patient privacy issues may instead contact the County Attorney at:

Goochland County Attorney's Office  
PO Box 10  
Goochland, Virginia 23063  
(804) 556-5877