

Twinsburg Fire Department

HIPAA Policies

Effective 4/14/03

TWINSBURG FIRE DEPARTMENT

TABLE OF CONTENTS

<u>TOPIC</u>	<u>Page</u>
What is HIPAA	3
Privacy Training	4
Electronic Patient Care Reports	6
Access, Security and Disclosure	7
Patient Requests for Protected Health Information	14
Patient Access Procedure	15
Patient Amendment Procedure	17
Patient Restriction Procedure	19
Accounting Policy	20
Patient Complaints Policy	21

TWINSBURG FIRE DEPARTMENT

What is HIPAA?

HIPAA is the Health Insurance Portability and Accountability Act of 1996. It requires all agencies that deal with medical records to keep patient information confidential.

The basic requirements of the privacy regulation apply to "protected health information" (PHI) which is defined as "individually identifiable health information" that is transmitted by electronic media, maintained in any medium that is defined as electronic media, or transmitted or maintained in any other form or medium. In effect, this includes all health information, whether electronic, paper or oral.

"Health information" means: any information, whether oral or recorded in any form or medium that:

- (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
- (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual.

Health information becomes "individually identifiable" if it identifies the individual or there is a reasonable basis to believe the information can be used to identify the individual.

TWINSBURG FIRE DEPARTMENT

Privacy Training

Purpose

To ensure that all staff members of Twinsburg Fire Department ("TFD"), including all employees, members, volunteers, students and trainees (collectively referred to as "staff members") who have access to patient information understand the organization's concern for the respect of patient privacy and are trained in TFD's policies and procedures regarding PHI.

Policy

1. All current staff will be required to undergo privacy training in accordance with the HIPAA Privacy Rule prior to the implementation date of the HIPAA Privacy Rule, which is April 14, 2003.
2. All new staff members will be required to undergo privacy training in accordance with the HIPAA Privacy Rule within a reasonable time upon association with the organization, as scheduled by the Privacy Officer (Asst. Chief Hartung).
3. All staff members will be required to undergo privacy training in accordance with the HIPAA Privacy Rule within a reasonable time after there is a material change to TFD's policies and procedures on privacy practices.

Procedure

1. The Privacy Training will be conducted by the Privacy Officer or his designee.
2. All attendees will receive copies of TFD's policies and procedures regarding privacy.
3. All attendees must attend the training in person and verify attendance and agreement to adhere to TFD's policies and procedures on privacy practices.
4. Training will be conducted using some or all the following: Video, Classroom with documentation, Power Point, Question and Answer Period.

5. Topics of the training will include a complete review of TFD's Policy on Privacy Practices and will include other information concerning the HIPAA Privacy Rule, such as, but not limited to, the following topic areas:
 - a. 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)
 - b. Description of protected health information (PHI)
 - c. Patient rights under the HIPAA Privacy Rule
 - d. Staff member responsibilities under the Privacy Rule
 - e. Role of the Privacy Officer and reporting employee and patient concerns regarding privacy issues
 - f. Importance of and benefits of privacy compliance
 - g. Consequences of failure to follow established privacy policies
 - h. Use of TFD's specific privacy forms
 - i. Handling of call cards

TWINSBURG FIRE DEPARTMENT

Electronic Patient Care Reports

Policy

To ensure that all staff members of Twinsburg Fire Department ("TFD") properly dispose of all "paper" used in the preparation of a patient care report (PCR) and to secure and restrict PCR accessibility.

Procedure

TFD maintains strict requirements on the security and access of all PCRs as well as the initial documentation created by the field providers in their preparation of a PCR.

1. All preliminary documentation used by a crewmember to assist in the creation or modification of a PCR is the sole property of TFD.
2. Each crewmember will be given a password to use TFD's computer systems.
3. No crewmember may disclose his/her password to any other crewmember.
4. Each crewmember is to access ONLY his/her PCRs unless directed otherwise by the Privacy Officer or as permitted by management.
5. No crewmember is to log onto any computer or password protected software under any user name other than his/her own.
6. A PCR may be amended by a crewmember upon approval by the Privacy Officer or Management.
7. Printed PCRs are to be placed in a secure place
8. All scratch paper used by a crewmember in the preparation of a PCR must be shredded immediately.
9. Inappropriate access or retention of PHI may result in disciplinary action, up to and including counseling, verbal reprimands, written reprimands, suspension, demotion and/or termination from the organization.

TWINSBURG FIRE DEPARTMENT

Access, Security and Disclosure

Purpose

To outline levels of access to Protected Health Information (PHI) for various staff members of Twinsburg Fire Department ("TFD") and to provide a policy and procedure on limiting access, disclosure, and use of PHI. To provide policies outlining patient rights and TFD's responsibilities in fulfilling patient requests. Security of PHI is everyone's responsibility.

Policy (Minimum Necessary Rule)

TFD retains strict requirements on the security, access, disclosure and use of PHI. Access, disclosure and use of PHI will be based on the role of the individual staff member in the organization, and should be only to the extent that the person needs access to PHI to complete necessary job functions.

When PHI is accessed, disclosed and used, the individuals involved will make every effort, except in patient care situations, to only access, disclose and use PHI to the extent that only the minimum necessary information is used to accomplish the intended purpose.

Patients may exercise their rights to access, amend, restrict, and request an accounting, as well as lodge a complaint with either TFD or the Secretary of the Department of Health and Human Services.

Procedure

Role Based Access

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

Job Title	Description of PHI to Be Accessed	Conditions of Access to PHI
EMT	Intake forms from dispatch, patient care reports	May access only as part of completion of a patient event and post-event activities and only while actually on duty
Paramedic	Intake forms from dispatch, patient care reports	May access only as part of completion of a patient event and post-event activities and only while actually on duty
Lieutenant	Intake forms from dispatch, patient care reports	May access only as part of completion of a patient event and post-event activities, as well as for quality assurance checks and corrective counseling of staff
Dispatcher	Intake forms, preplanned CAD information on patient address	May access only as part of completion of an incident, from receipt of information necessary to dispatch a call, to the closing out of the incident and only while on duty
Administrative Assistant	Intake forms from dispatch, patient care reports	May access only as a part of record keeping and distribution of information to individuals, insurance companies or lawyers after approved by privacy officer
Computer Administrators		May access only as a part of maintaining the operating system functions
Department Managers		May access only to the extent necessary to monitor compliance, accomplish appropriate supervision and management of personnel and report to state agencies

Access to PHI is limited to the above-identified persons only, and to the identified PHI only, based on the Department'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 expressly permitted by Department policy or approved by the Privacy Officer.

Disclosures to and Authorizations from the Patient

You are not required to limit your 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, any mutual aid provider, your 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. In addition, disclosures authorized by the patient are exempt from the minimum necessary requirements unless the authorization to disclose PHI is requested by the Department.

Authorizations received directly from third parties, such as Medicare, or other insurance companies, which direct you to release PHI to those entities, are not subject to the minimum necessary standards.

For example, if we have a patient's authorization to disclose PHI to Medicare, Medicaid or another health insurance plan for claim determination purposes, the Department 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 of when the minimum necessary rule applies is when your Department conducts quality assurance activities. In most situations it is not necessary to disclose certain patient information such as the patient's name, address, social security number, all PHI of the treated patient, in order to conduct a call review. This sensitive information should be redacted or blacked out from the PCR being used as a Q/A example.

Department Requests for PHI

If the Department needs to request PHI from another health care provider on a routine or recurring basis, we must limit our requests to only the reasonably necessary information needed for the intended purpose, as described below. For requests not

covered below, you must make this determination individually for each request and you should consult your supervisor for guidance. For example, if the request is non-recurring or non-routine, like making a request for documents via a subpoena, we must review the request to make sure it covers only the minimum necessary PHI to accomplish the purpose of the request.

Holder of PHI	Purpose of Request	Information Reasonably Necessary to Accomplish Purpose
Skilled Nursing Facilities	To have adequate patient records to determine medical necessity for service and to properly bill for services provided	Patient face sheets, discharge summaries, Physician Certification Statements and Statements of Medical Necessity, Mobility Assessments
Hospitals	To have adequate patient records to determine medical necessity for service and to properly bill for services provided	Patient face sheets, discharge summaries, Physician Certification Statements and Statements of Medical Necessity, Mobility Assessments
Mutual Aid Ambulance or Paramedic Services	To have adequate patient records to conduct joint billing operations for patients mutually treated/transported by the Department	Patient care reports

For all other requests, determine what information is reasonably necessary for each on an individual basis.

Incidental Disclosures

The Department 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 staff needs to be sensitive about the importance of maintaining the confidence and security of all material we create or use that contains patient care information. Coworkers and other staff members should not have access to information that is not necessary for the staff 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.

However, 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. Pay attention to who is within earshot when you make verbal statements about a patient's health information, and follow some of these common sense procedures for avoiding accidental or inadvertent disclosures:

Verbal Security

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 area before engaging in discussion.

Garage Areas: Staff members should be sensitive to the fact that members of the public and other agencies may be present in the garage and other easily accessible areas. Conversations about patients and their health care should not take place in areas where those without a need to know are present.

Other Areas: Staff members should only discuss patient care information with those who are involved in the care of the patient, regardless of your physical location. You should be sensitive to your level of voice and to the fact that others may be in the area when you are speaking. 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, you should be free to discuss all aspects of the patient's medical condition, treatment provided, and any of their health information you may have in your possession with others involved in the care of the patient.

Physical Security

Patient Care and Other Patient or Billing Records: Patient care reports should be stored in safe and secure areas. 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.

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

Computers and Entry Devices: Computer access terminals and other remote entry devices such as PDAs and laptops should be kept secure. Access to any computer device should be by password only. Staff 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. All remote devices such as laptops and PDAs should remain in the physical possession of the individual to whom it is assigned at all times.

Penalties for Violation

The Department takes its responsibility to safeguard patient information very seriously. There are significant legal penalties against companies and individuals that do not adhere to the laws that protect patient privacy.

Staff members who do not follow our policies on patient privacy will be subject to disciplinary action, up to and including counseling, verbal reprimands, written reprimands, suspension, demotion and/or termination from the organization. The Department shall make every effort to provide remedial education and training as to our policies and procedures when there is a first time violation of our policies.

Questions About This Policy or Any Privacy Issues

The Department has appointed a Privacy Officer to oversee our policies and procedures on patient privacy and to monitor compliance. The Privacy Officer is also available to you for consultation on any issues or concerns you have about how our Department deals with protected health information. You should feel free to contact the Privacy Officer at any time with your questions or concerns.

The Department will not retaliate against any staff member who expresses a good concern or complaint about any policy or practice related to the safeguarding of patient information and the Department's legal obligations to protect patient privacy.

If the Privacy Officer is unavailable, contact the Fire Chief for assistance.

TWINSBURG FIRE DEPARTMENT

Patient Requests for Protected Health Information

Purpose

To ensure that all patients treated by TFD are apprised of their rights with regard to PHI and that TFD provides the necessary tools to facilitate patient requests.

Policy - Notice of Privacy Practices (NPP)

TFD field providers will furnish a copy of TFD's NPP to the patient at or prior to treatment in non-emergency situations and as circumstances permit after treatment in an emergency. In non-emergency situations only, field personnel should attempt to get a signed acknowledgement from patient or note why a signature was not obtained.

Procedure - Non-emergency Transport

1. Provide a copy of the NPP to the patient.
2. Indicate on your trip sheet that a copy has/has not been given to the patient, family member or with hospital staff.
3. Have the patient sign an Authorization/Acknowledgement form.
4. An authorized personal representative of the patient may sign on the patient's behalf.
5. If no signature can be obtained, please explain reason.

Procedure - Emergency Transport

1. Provide a copy of the NPP to the patient.
2. Indicate on your trip sheet that a copy has/has not been given to the patient, family member or with hospital staff.
3. You do not need the patient to acknowledge receipt of NPP.
4. Attempt to obtain any other necessary signatures if possible.
5. If unable to obtain patient's signature, please provide reason.

Procedure - Refusals of Care

1. Provide a copy of the NPP to the patient.
2. Indicate on your trip sheet that a copy has/has not been given to the patient, family member or with hospital staff.
3. Have the patient sign the Refusal form.

4. Have the patient sign an Acknowledgement form.
5. An authorized personal representative of the patient may sign on the patient's behalf.
6. If no signature can be obtained, please explain reason.

Policy - Patient Access, Amendment or Restriction to PHI

Only information contained in the Designated Record Set (DRS) outlined in this policy is to be provided to patients who request access, amendment and restriction on the use of their PHI in accordance with the Privacy Rule and the Privacy Practices of TFD.

Procedure - Patient Access

1. Upon presentation to the department headquarters, the patient or appropriate representative will complete a Request for Access Form.
2. The Department employee must verify the patient's identity, and if the requestor is not the patient, the name of the individual and reason that the request is being made by this individual. The use of a driver's license, social security card, or other form of government-issued identification is acceptable for this purpose.
3. The completed form will be presented to the Privacy Officer for action.
4. The Privacy Officer will act upon the request within 30 days, preferably sooner. Generally, the Department 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 TFD 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 TFD could not respond within the time frame and in that case TFD 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 below and

may make a copy of the PHI contained in the DRS upon verbal or written request.

7. The City of Twinsburg will establish a reasonable charge for copying PHI for the patient or appropriate representative.
8. Patient access may be denied for the reasons listed below, and in some cases the denial of access may be appealed to TFD for review.
9. The following are reasons to deny access to PHI that are not subject to review and are final and may not be appealed by the patient:
 - a. If the information the patient requested was compiled in reasonable anticipation of, or use in, a civil, criminal or administrative action or proceeding;
 - b. If the information the patient 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.
10. The following reasons to deny access to PHI are subject to review and the patient may appeal the denial:
 - a. If a licensed health care professional 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 protected health information makes reference to another person (other than a health care provider) and a licensed health professional 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 a licensed health professional has determined, in the exercise of professional judgment, that access by you

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 Privacy Officer.
 - e. TFD will designate a licensed health professional, who was not directly involved in the denial, to review the decision to deny the patient access. TFD 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. TFD 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 TFD's determination.
- 11. Access to the actual files or computers that contain the DRS that may be accessed by the patient or requestor should not be permitted. Rather, 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 TFD staff member. UNDER NO CIRCUMSTANCES SHOULD ORIGINALS OF PHI LEAVE THE PREMISES.
 - 12. If the patient or requestor would like to retain copies of the DRS provided, then TFD may charge a reasonable fee for the cost of reproduction.
 - 13. Whenever a patient or requestor accesses a DRS, a note should be maintained in a log book 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.
 - 14. 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.

Procedure - Patient Amendment

15. The patient or appropriate requestor may only request amendment to PHI contained in the DRS. A Request for Amendment Form must be accompanied by any request for amendment.
16. TFD must act upon a Request for Amendment within 60 days of the request. If TFD 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.
17. All requests for amendment must be forwarded immediately to the Privacy Officer for review.

Granting Requests for Amendment

18. If the Privacy 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.
19. There must be written permission provided by the patient so that TFD may notify the persons with whom the amendments need to be shared. TFD 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.
20. The patient must identify individuals who may need the amended PHI and sign the statement in the Request for Amendment form giving TFD permission to provide them with the updated PHI.
21. TFD 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 TFD to the designated record set.

Denial of Requests for Amendment

22. TFD may deny a request to amend PHI for the following reasons: 1) if the originator of the record is no longer available; 2) if TFD did not create the PHI at issue; 3) if the information is not part of the patient care

- record; 4) if the information is accurate and complete;
5) if the information received from someone else under a promise of confidentiality.
23. TFD must provide a written denial, and the denial must be in plain language stating 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.
 24. 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 TFD's option, a summary of the disagreement will be appended, along with the rebuttal statement of TFD.
 25. If TFD 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.

Procedure - Patient Restriction

26. The patient may request a restriction on the use and disclosure of their PHI.
27. TFD is not required to agree to any restriction, and given the emergent nature of our operation, we generally will not agree to a restriction.
28. ALL REQUESTS FOR RESTRICTION ON USE AND DISCLOSURE OF PHI MUST BE SUBMITTED IN WRITING ON THE APPROVED DEPARTMENT FORM. ALL REQUESTS WILL BE REVIEWED AND DENIED OR APPROVED BY THE PRIVACY OFFICER.
29. If TFD agrees to a restriction, we 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, TFD may use the restricted PHI or may disclose such PHI to another health care provider to provide treatment to the individual.

30. The agreement to restrict PHI will be documented to ensure that the restriction is followed.
31. 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 TFD as long as TFD notifies the patient that PHI created or received after the restriction is removed is no longer restricted. PHI that was restricted prior to TFD voiding the restriction must continue to be treated as restricted PHI.

Policy - Accounting

To provide guidance to management and staff concerning the patient's right to an Accounting and the types of uses and disclosures of PHI for which TFD is required to document.

Procedure

1. All patient records will be kept by TFD for a period of six (6) years from the date of service.
2. All patient accounting requests should be received directly from a patient or personal representative.
3. TFD will provide a list of uses and disclosures of the patient's PHI, made by TFD or by a Business Associate on TFD's behalf, for the last six (6) years or to the extent that TFD has maintained that patient's information if less than six (6) years.
4. All uses and disclosures of a patient's PHI, made by TFD, must be documented for accounting purposes except:
 - a. Disclosures to carry out treatment, payment and health care operations;
 - b. For national security or intelligence purposes;
 - c. Uses and disclosures incident to an unaccountable use or disclosure;
 - d. That occurred prior to the compliance date.

5. 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.

Policy - Patient Complaints

Patients have the right to complain to the Department about any concerns they may have concerning patient privacy. Any patient or family member who expresses a concern or complaint to you should be directed to contact the Privacy Officer. The Privacy Officer is responsible for receiving, investigating, and documenting all complaints from patients concerning patient privacy issues.