The Westerville Division of Fire

HIPAA Compliance Policy

Effective 14 April 2003

This Policy Manual contains the methodology the Westerville Division of Fire will utilize to meet HIPAA Regulations

Table of Contents
Forms, Policies and Documents

The Westerville Division of Fire
List of Forms and Policies

Required Forms and Policies

Required Forms

The Westerville Division of Fire will utilize the following to comply with the various elements of the Privacy Rule:

- Notice of Privacy Practices

  Required to provide the patient with a copy of this notice. The notice should be provided to the patient at the time of service or before. If we are unable to provide the notice at the time of service, as in an emergency call, we should provide the notice as soon as we reasonably can do so after the service is provided.

- Acknowledgement of Receipt of Notice of Privacy Practices

  Required, except in emergency situations, to obtain an acknowledgement of receipt of the Notice of Privacy Practices. There is no required form for the acknowledgement, and the acknowledgement may be included as part of the signature authorization form used for billing purposes.

- Authorization Form

  The patient must provide written authorization for the use or disclosure of PHI that is not related to treatment, payment or operations. These situations will generally be few in number for the typical EMS service, since most exchanges of PHI will be between the EMS service, hospital, or other medical facility, and those disclosures are permitted without the need for a written authorization from the patient.

- Patient Accounting Log

  We are required to maintain a log of the uses and disclosures of PHI that are not related to treatment, payment and operations. This log will be used when a patient requests an accounting of PHI disclosures.

- Patient Accounting Form

  We are required to provide the patient with a list of disclosures and uses of PHI that were not related to treatment, payment or operations.

- List of Designated Privacy Officials

The Privacy Rule requires that we maintain a list of those responsible for compliance, including the designation of a privacy officer.

Required Policies

The Westerville Division of Fire will utilize the following to comply with the administrative requirements of the Privacy Rule:

- Policy on Patient Access, Amendment and Request for Restriction on Use of Protected Health Information

In this policy, we identify the classes of employees who may have access to the entire medical record, with justification for that access. Members of the classes of employees who have full access per the policy & procedure are free to use and disclose all information between and among each other as required for treatment purposes.

- Policy on Designated Record Sets (DRS)

  We need to identify what records are included as PHI that the patient may have access to. We are only required to provide access to the records that we identify as containing PHI. Medical, billing and other records used to make decisions about the patient must be included in the Designated Record Sets (DRS).

- Policy on Confidentiality and Dissemination of Patient Information and Staff Verification

  This policy spells out staff expectations and obligations and provides for disciplinary action for violation of the privacy practices of the Department.

- Policy on Security, Levels of Access and Limiting Disclosure and Use of PHI

  The Privacy Rule focus is on limiting access and use of PHI to only the amount necessary for the individual staff member to complete his or her job. This is called "role based access" and this type of policy helps communicate the importance of being sensitive to the amount of PHI to which each staff member has access.

Beneficial Forms and Policies

Beneficial Forms

The following forms are highly beneficial to our HIPAA Compliance activities. Some of the forms deal with required areas where the Privacy Rule does not specify that a particular form must be used, but, nonetheless, a form may be most helpful to ensure compliance:

- Patient Request for Access Form

This allows us to keep track of access requests and to respond to those requests.

- Denial of Request for Access Form

  This form allows us to provide the patient with the Department's denial of patient's request for access to PHI.

- Request for Amendment of PHI Form

  This form allows us to more smoothly process a patient's request to amend PHI.

- Acceptance of Request for Amendment of PHI Form

  This form allows us to document the acceptance of a patient's request for amendment so that we can properly keep track of those requests.

- Denial of Request for Amendment Form

  This form allows us to properly deal with denials of a patient's request for amendment of PHI.

- Patient Request for Restriction Form

  This form allows us to respond to a request from a patient to restrict our use and disclosure of PHI. It is generally recommended that EMS providers deny these requests, given the nature of EMS and the fact that the Privacy Rule permits denial of these requests for whatever reason.

- Password Authorization Form

  Although the HIPAA Security Rule is not yet finalized, under the Privacy Rule, covered entities must implement reasonable administrative safeguards to protect PHI from unnecessary use and disclosure. The use of passwords that are protected and changed regularly, helps ensure compliance with the Privacy Rule, and is also considered a basic element of security in the data processing field.

- Procedure for Filing Complaints About Privacy Practices

  Since the Privacy Rule requires that a covered entity advise patients of their right to complain about privacy practices, this from helps ensure compliance with this requirement.

- Log for Processing Complaints About Privacy Practices

A record of complaints will be kept to help guide and direct HIPAA compliance activities, and this log, which should be kept by the designated privacy officer, should aid in this process.

- Privacy Officer Job Description

  The Privacy Rule requires that a privacy officer be designated by a covered entity, and this job description helps to quantify the roles and responsibilities of the compliance officer.

- Job Description Language for Compliance with Privacy Practices

  Every staff member, whether paid or volunteer, should comply with the privacy practices of the organization. This language has been added to existing position descriptions to indicate the importance of privacy and confidentiality for all staff members.

- Privacy Training Record Form

  This form helps us keep track of the HIPAA compliance training, which is required under the Privacy Rule. Training records should be maintained for six years.

- Confidentiality Language for Vendors Who Are Not Business Associates

  Some vendors may not be business associates since they do not perform a function on our behalf that deals with PHI. This language may be used to incorporate privacy protection in ancillary vendor contracts not subject to the business associate requirements.

<u>Beneficial Policies</u>

The following policies are highly beneficial to our HIPAA Compliance activities. Some of the policies deal with required areas where the Privacy Rule does not specify that a policy be used, but, nonetheless, a policy may be most helpful to ensure compliance:

- Policy on Use of Computer and Information Systems and Equipment

  An important aspect of HIPAA compliance in EMS deals with security of computer equipment, since the industry relies so heavily on computerization. It is important that fundamental aspects of computer security be in place at all times to ensure the protection and integrity of all PHI. This policy includes dealing with the use of remote data entry devices, which has become a popular use of computerization in EMS.

- Policy on Privacy Training

Since the Privacy Rule mandates training of staff by all covered entities, this policy helps establish the importance of Department focus on this essential HIPAA compliance activity.

- Policy on Medical Records of Employees

  Certain employment records related to workers' compensation and other areas involving employees are not considered PHI, while records of employees who receive ambulance service from your organization are protected PHI. This policy deals with the distinction between the two.

The Westerville Division of Fire
Notice of Privacy Practices

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

As an essential part of our commitment to you, The Westerville Division of Fire maintains the privacy of certain confidential health care information about you, known as Protected Health Information or PHI. We are required by law to protect your health care information and to provide you with the attached Notice of Privacy Practices.

The Notice outlines our legal duties and privacy practices respect to your PHI. It not only describes our privacy practices and your legal rights, but lets you know, among other things, how The Westerville Division of Fire is permitted to use and disclose PHI about you, how you can access and copy that information, how you may request amendment of that information, and how you may request restrictions on our use and disclosure of your PHI.

The Westerville Division of Fire is also required to abide by the terms of the version of this Notice currently in effect. In most situations we may use this information as described in this Notice without your permission, but there are some situations where we may use it only after we obtain your written authorization, if we are required by law to do so.

We respect your privacy, and treat all health care information about our patients with care under strict policies of confidentiality that all of our staff are committed to following at all times.

PLEASE READ THE ATTACHED DETAILED NOTICE. IF YOU HAVE ANY QUESTIONS ABOUT IT, PLEASE CONTACT _Deputy Chief Ingles, OUR PRIVACY OFFICER, AT __614-901-6600.

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.

Purpose of this Notice: The Westerville Division of Fire 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. This Notice describes your legal rights, advises you of our privacy practices, and lets you know how The Westerville Division of Fire is permitted to use and disclose PHI about you.

The Westerville Division of Fire is also required to abide by the terms of the version of this Notice currently in effect. In most situations we may use this information as described in this Notice without your permission, but there are some situations where we may use it only after we obtain your written authorization, if we are required by law to do so.

Uses and Disclosures of PHI: The Westerville Division of Fire 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 are:

For treatment. This includes such things as verbal and written information that we obtain about you and use pertaining to your medical condition and treatment provided to you by us and other medical personnel (including doctors and nurses who give orders to allow us to provide treatment to you). It also includes information we give to other health care personnel to whom we transfer your care and treatment, and includes transfer of PHI via radio or telephone to the hospital or dispatch center as well as providing the hospital with a copy of the written record we create in the course of providing you with treatment and transport.

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 organizing your PHI and submitting bills to insurance companies (either directly or through a third party billing Department), management of billed claims for services rendered, medical necessity determinations and reviews, utilization review, and collection of 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, obtaining legal and financial services, conducting business planning, processing grievances and complaints, creating reports that do not individually identify you for data collection purposes, fundraising, and certain marketing activities.

Fundraising. We may contact you when we are in the process of raising funds for The Westerville Division of Fire, or to provide you with information about our annual subscription program.

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 for other information about alternative services we provide or other health-related benefits and services that may be of interest to you.

Use and Disclosure of PHI Without Your Authorization. The Westerville Division of Fire is permitted to use PHI *without* your written authorization, or opportunity to object in certain situations, including:

- For The Westerville Division of Fire's use in treating you or in obtaining payment for services provided to you or in other health care operations;
- For the treatment activities of another health care provider;
- To another health care provider or entity for the payment activities of the provider or entity that receives the information (such as your hospital or insurance Department);
- To another health care provider (such as the hospital to which you are transported) for the health care operations activities of the entity that receives the information as long as the entity receiving the information has or has had a relationship with you and the PHI pertains to that relationship;
- For health care fraud and abuse detection or for activities related to compliance with the law;
- 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. We may also disclose health information to your family, relatives, or friends if we infer from the circumstances that you would not object. For example, we may assume you agree to our disclosure of your personal health information to your spouse when your spouse has called the ambulance for you. In situations where you are not capable of objecting (because you are not present or due to your incapacity or medical emergency), we may, in our professional judgment, determine that a disclosure to your family member, relative, or friend is in your best interest. In that situation, we will disclose only health information relevant to that person's involvement in your care. For example, we may inform the person who accompanied you in the ambulance that you have certain symptoms and we may give that person an update on your vital signs and treatment that is being administered by our ambulance crew;
- To a public health authority in certain situations (such as reporting a birth, death or disease as required by law, as part of a public health investigation, to report child or adult abuse or neglect or domestic violence, to report adverse events such as product defects, or to notify a person about exposure to a possible communicable disease as required by law;
- 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 or other legal process;
- For law enforcement activities in limited situations, such as when there is a warrant for the request, or when the information is needed to locate a suspect or stop a crime;
- 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 and health information will be released only when there is a minimal risk to your privacy and adequate safeguards are in place in accordance with the law;
- We may 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 only be made with your written authorization, (the authorization must specifically identify the information we seek to use or disclose, as well as when and how we seek to use or disclose it). **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 the protection of your PHI, including:

The right to access, copy or inspect your PHI. This means you may come to our offices and 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 you may appeal certain types of denials.

We have available forms to request access to your PHI and we will provide a written response if we deny you access and let you know your appeal rights. If you wish to inspect and copy your medical information, you should contact the privacy officer listed at the end of this Notice.

The right to amend your PHI. You have the right to ask us to amend written medical information that we may have about you. 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. If you wish to request that we amend the medical information that we have about you, you should contact the privacy officer listed at the end of this Notice.

The right to request an accounting of our use and disclosure of your PHI. You may request an accounting from us of certain disclosures of your medical information that we have made in the last six years prior to the date of your request. We are not required to give you an accounting of information we have used or disclosed for purposes of treatment, payment or health care operations, or when we share your health information with our business associates, like our billing Department or a medical facility from/to which we have transported you.

We are also not required to give you an accounting of our uses of protected health information for which you have already given us written authorization. If you wish to request an accounting of the medical information about you that we have used or disclosed that is not exempted from the accounting requirement, you should contact the privacy officer listed at the end of this Notice.

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 your medical information that we have about you for treatment, payment or health care operations, or to restrict the information that is provided to family, friends and other individuals involved in your health care. But if you request a restriction and the information you asked us to restrict is needed to provide you with emergency treatment, then we may use the PHI or disclose the PHI to a health care provider to provide you with emergency treatment. The Westerville Division of Fire is not required to agree to any restrictions you request, but any restrictions agreed to by The Westerville Division of Fire are binding on The Westerville Division of Fire.

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 and make the Notice available electronically through the 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: The Westerville Division of Fire 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 the Privacy Officer identified below.

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 the privacy officer listed at the end of this Notice. Individuals will not be retaliated against for filing a complaint.

If you have any questions or if you wish to file a complaint or exercise any rights listed in this Notice, please contact: Deputy Chief Ingles @614-901-6600 or beingles@westerville.org.

Effective Date of the Notice: [6-30-03]

The Westerville Division of Fire
Acknowledgment of Receipt of Notice of Privacy Practices

[NOTE: YOU NEED ONLY HAVE THE PATIENT SIGN EITHER THE LOG SHEET, THE SEPARATE NOTICE, OR THE ASSIGNMENT OF BENEFITS FORM WHICH CONTAINS THE ACKNOWLEDGEMENT.]

I hereby acknowledge that I have been provided with a copy of The Westerville Division of Fire's Notice of Privacy Practices on this date.

_____ _____

Date Signature

_____

PRINT NAME OF PATIENT

_____

Street Address

_____

City, State and Zip Code

The Westerville Division of Fire
Log for Recording Acknowledgement of
Receipt of Notice of Privacy Practices

YOU NEED ONLY HAVE THE PATIENT SIGN THE LOG SHEET, THE SEPARATE NOTICE, OR THE ASSIGNMENT OF BENEFITS FORM THAT CONTAINS THE ACKNOWLEDGEMENT.

NOTICE: SIGNATURE VERIFICATION REQUIRED

My signature below indicates my acknowledgment of receipt of The Westerville Division of Fire's Notice of Privacy Practices:

Date	Name of Patient	Signature	Relationship ("self" if patient signs)

The Westerville Division of Fire
Assignment of Benefits Authorization, Responsibility for Payment and Acknowledgement of Receipt of Notice of Privacy Practices

NOTE: YOU NEED ONLY HAVE THE PATIENT SIGN THE LOG SHEET, THE SEPARATE NOTICE, OR THE ASSIGNMENT OF BENEFITS FORM THAT CONTAINS THE ACKNOWLEDGEMENT.

BILLING AUTHORIZATION, RESPONSIBILITY FOR PAYMENT AND RECEIPT OF NOTICE OF PRIVACY RIGHTS

I understand that I am financially responsible for the services provided to me by The Westerville Division of Fire ("WTFD") regardless of insurance coverage. I request that payment of authorized Medicare or other insurance benefits be made on my behalf to WTFD for any services provided to me by WTFD. I authorize and direct any holder of medical information or documentation about me to release to the Centers for Medicare and Medicaid Services and its carriers and agents, as well as to WTFD and its billing agents and any other payers or insurers, any information or documentation needed to determine these benefits or benefits payable for any services provided to me by WTFD, now or in the future. I agree to immediately remit to WTFD any payments that I receive directly from any source for the services provided to me and I assign all rights to such payments to The Westerville Division of Fire.

I also acknowledge that I have received a copy of the The Westerville Division of Fire Notice of Privacy Practices. A copy of this form is as valid as the original.

_____ Date:_____
Patient Signature

_____ _____
Patient Representative's Signature Relationship to Patient

Patient unable to sign because:

_____

THE WESTERVILLE DIVISION OF FIRE

Policy on Patient Access, Amendment and Restriction on Use of Protected Health Information

Purpose:

Under the HIPAA Privacy Rule, individuals have the right to access and to request amendment or restriction on the use of their protected health information, or PHI, and restrictions on its use that is maintained in "designated record sets," or DRS. (See policy on Designated Record Sets).

To ensure that The Westerville Division of Fire only releases the PHI that is covered under the Privacy Rule, this policy outlines procedures for requests for patient access, amendment, and restriction on the use of PHI.

This policy also establishes the procedure by which patients or appropriate requestors may access PHI, request amendment to PHI, and request a restriction on the use of PHI.

Policy

Only information contained in the 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 The Westerville Division of Fire.

Procedure

Patient Access:

1. Upon presentation to the business office, 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 this individual is making the request. 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 the Department 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 the Department could not respond within the time frame and in that case the Department may extend the response time by an additional 30 days.

6. Upon approval of access, 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 business office 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 the Department 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 us 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. The Department will designate a licensed health professional, who was not directly involved in the denial, to review the decision to deny the patient access. The Department 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. The Department 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 the Department'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 Department 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 the Department may charge a reasonable fee for the cots 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.

Requests for Amendment to PHI

15. The patient or appropriate requestor may only request amendment to PHI contained in the DRS. The "Request for Amendment of PHI" Form must be accompanied with any request for amendment.

16. The Department must act upon a Request for Amendment within 60 days of the request. If the Department 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.

Granting Requests for Amendment

17. All requests for amendment must be forwarded immediately to the Privacy Officer for review.

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 that the Department may notify the persons with which the amendments need to be shared. The Department 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 the Department permission to provide them with the updated PHI.

21. The Department 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 the Department to the designated record set.

Denial of Requests for Amendment

22. The Department may deny a request to amend PHI for the following reasons: 1) If the Department did not create the PHI at issue; 2) if the information is not part of the DRS; or 3) the information is accurate and complete.

23. The Department 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.

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 the Department's option, a summary of the disagreement will be appended, along with the rebuttal statement of the Department.

25. If the Department 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

26. The patient may request a restriction on the use and disclosure of their PHI.

27. The Department 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 the Department 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, the Department 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. The Department may also terminate a current restriction as long as the Department notifies the patient that PHI created or received after the restriction is removed is no longer restriction. PHI that was restricted prior to the Department voiding the restriction must continue to be treated as restricted PHI.

The Westerville Division of Fire

Policy on Procedure for Request for Amendment to Protected Health Information

Purpose

To provide consistent guidelines for The Westerville Division of Fire staff so that they may assist a patient in amending the protected health information (PHI) of their patient care record in accordance with their rights under the federal Privacy Regulations.

Policy

An individual has the right to amend his/her patient care records, as long as The Westerville Division of Fire maintains their protected health information, except in the following circumstances:

- The originator of the record is no longer available.
- The information the patient is requesting to amend was not created by The Westerville Division of Fire
- The information is not part of the patient care record
- The information is accurate and complete
- The information would not be available for inspection as provided by law, and therefore The Westerville Division of Fire is not required to consider an amendment. This exception applies to information compiled in anticipation of a legal proceeding
- Information received from someone else under a promise of confidentiality

Procedure

1. Confirm the identity of requestor or legal representative. If the requestor is legal representative, ask for legal proof of their representative status;

2. The patient must fill out the Request for Amendment of Health Information form completely;

3. The Department, with the assistance of legal counsel, will act on the request for amendment within 60 days of the request;

4. If the Department agrees with the amendment,

    a. Then the record will be amended;

    b. The Department will then notify the individual of the agreement to amend the record;

c. Copies of the amended record will be provided to our business associates, facilities to or from which we have transported the patient, and others involved in the patient's treatment.

5. If the Department denies the request for amendment,

a. Then the individual that requested the amendment will be notified of the denial, and the reason for the denial in writing;

b. A statement will be given to the individual that he/she may submit a short written statement disagreeing with the denial, and how the individual may file such a statement;

c. A statement will be given to that individual that he/she may, if they do not wish to submit a statement of disagreement, that they may request that the Request for Amendment and the denial become a permanent part of their medical record;

d. A statement that the individual may complain to the Privacy Officer of the Department at 614-901-6600, or to the federal agency that oversees enforcement of the federal Privacy Rule, the Department of Health and Human Services;

6. All documentation pertaining to the request for amendment will be kept in the medical record.

The Westerville Division of Fire
Policy on Designated Record Sets

Purpose

To ensure that The Westerville Division of Fire releases Protected Health Information (PHI) in accordance with the Privacy Rule, this policy establishes a definition of what information should be accessible to patients as part of the 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 records that are created or used by the Department to make decisions about the patient.

Policy

The DRS should only include HIPAA covered PHI, and should not include information used for the operational purposes of the organization, such as quality assurance data, accident reports, and incident reports. The type of information that should be included in the DRS is medical records and billing records.

Procedure

The Designated Record Set

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

    a. The patient care report or PCR 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 and/or attached to the PCR.

    b. The electronic claims records or other paper records of submission of actual claims to Medicare or other insurance companies.

    c. 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.

    d. 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.

e. 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.

2. The DRS also include copies of records created by other service providers and other health care providers such as first responder units, assisting ambulance services, air medical services, nursing homes, hospitals, police departments, coroner's office, etc., that are used by the Department as part of treatment and payment purposes related to the patient.

The Westerville Division of Fire
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* _____

The Westerville Division of Fire
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 The Westerville Division of Fire 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. ____ 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;

4. ____ 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;

5. ____ The request for access is made by you as a personal representative of the individual about whom you are 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.

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:

Deputy Chief Ingles
400 W. Main St.
Westerville, Ohio 43081
614-901-6600

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,

Deputy Chief Ingles
Privacy Officer
The Westerville Division of Fire

The Westerville Division of Fire
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.

____ Name
____ Billing Address
____ Mailing Address
____ Current Medical Condition
____ Past Medical History
____ Current Medications
____ Allergies
____ Marital Status
____ Surrogate Decision Maker
____ Organ Donor
____ Other: Please describe
_____
_____
_____

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

The Westerville Division of Fire, 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. The Westerville Division of Fire 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 The Westerville Division of Fire based on existing protected information until such time that the amendments you have made are effective.

Patient Signature: _____ *Date:* _____

The Westerville Division of Fire
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
Deputy Chief Ingles
Privacy Officer
The Westerville Division of Fire
400 W. Main St.
Westerville, Ohio 43081
614-901-6600

Sincerely,

Deputy Chief Ingles

By my signature below, I hereby agree to allow The Westerville Division of Fire to provide amended PHI that it may have about me to the following persons, and to others who The Westerville Division of Fire 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

The Westerville Division of Fire
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: WE MUST GIVE A PLAIN LANGUAGE REASON FOR THE DENIAL. WE MAY DENY THE REQUEST FOR AMENDMENT IF: 1) WE 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 privacy officer, Deputy Chief Ingles, at 400 W. Main St. Westerville, Ohio 43081.

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,

Deputy Chief Ingles
Privacy Officer
The Westerville Division of Fire

The Westerville Division of Fire
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, prior to the date of the request, from The Westerville Division of Fire. **NOTE: The Westerville Division of Fire 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

THE WESTERVILLE DIVISION OF FIRE
Accounting Log for Disclosures of Protected Health Information

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

The Westerville Division of Fire
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. **The Westerville Division of Fire is not required to agree to any restrictions requested by the patient, however any restrictions agreed to by The Westerville Division of Fire are binding on The Westerville Division of Fire.**

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

_____

_____

_____

_____

Signature _____ *Date*_____

FOR FIRE DEPARTMENT USE ONLY

DATE REC'D _____

REQUEST ACCEPTED _____

REQUEST DENIED _____

DATE _____

REVIEWING OFFICIAL _____

NOTICE TO PT _____

COMMENTS: _____

_____

The Westerville Division of Fire
Policy on Confidentiality and Dissemination of Patient Information and Uniformed Staff Member Verification

Given the nature of our work, it is imperative that we maintain the confidence of patient information that we receive in the course of our work. The Westerville Division of Fire prohibits the release of any patient information to anyone outside the organization unless required for purposes of treatment, payment, or health care operations, and discussions of Protected Health Information (PHI) within the organization should be limited. Acceptable uses of PHI within the organization include, but are not limited to, exchange of patient information needed for the treatment of the patient, billing, and other essential health care operations, peer review, internal audits, and quality assurance activities.

I understand that The Westerville Division of Fire provides services to patients that are private and confidential and that I am a crucial step in respecting the privacy rights of The Westerville Division of Fire's patients. I understand that it is necessary, in the rendering of The Westerville Division of Fire services, that patients provide personal information and that such information may exist in a variety of forms such as electronic, oral, written or photographic and that all such information is strictly confidential and protected by federal and state laws.

I agree that I will comply with all confidentiality policies and procedures set in place by The Westerville Division of Fire during my entire employment or association with The Westerville Division of Fire. If I, at any time, knowingly or inadvertently breach the patient confidentiality policies and procedures, I agree to notify the Privacy Officer of The Westerville Division of Fire immediately. In addition, I understand that a breach of patient confidentiality may result in disciplinary action as defined in The Westerville Division of Fire employee manual and/or labor contract. Upon termination of my employment or association for any reason, or at any time upon request, I agree to return any and all patient confidential information in my possession. This is not a contract for continued employment.

I have read and understand all privacy policies and procedures that have been provided to me by The Westerville Division of Fire. I agree to abide by all policies or be subject to disciplinary action, which may include verbal or written warning, suspension, or termination of employment or of any membership or association with The Westerville Division of Fire. This is not a contract of employment and does not alter the nature of the existing relationship between The Westerville Division of Fire and me.

Signature: _____ *Date:*_____ *Printed*

Name:_____

The Westerville Division of Fire
Policy on Confidentiality and Dissemination of Patient Information and Civilian Staff Member Verification

Given the nature of our work, it is imperative that we maintain the confidence of patient information that we receive in the course of our work. The Westerville Division of Fire prohibits the release of any patient information to anyone outside the organization unless required for purposes of treatment, payment, or health care operations, and discussions of Protected Health Information (PHI) within the organization should be limited. Acceptable uses of PHI within the organization include, but are not limited to, exchange of patient information needed for the treatment of the patient, billing, and other essential health care operations, peer review, internal audits, and quality assurance activities.

I understand that The Westerville Division of Fire provides services to patients that are private and confidential and that I am a crucial step in respecting the privacy rights of The Westerville Division of Fire's patients. I understand that it is necessary, in the rendering of The Westerville Division of Fire services, that patients provide personal information and that such information may exist in a variety of forms such as electronic, oral, written or photographic and that all such information is strictly confidential and protected by federal and state laws.

I agree that I will comply with all confidentiality policies and procedures set in place by The Westerville Division of Fire during my entire employment or association with The Westerville Division of Fire. If I, at any time, knowingly or inadvertently breach the patient confidentiality policies and procedures, I agree to notify the Privacy Officer of The Westerville Division of Fire immediately. In addition, I understand that a breach of patient confidentiality may result in disciplinary action as defined in the The Westerville Division of Fire employee manual. Upon termination of my employment or association for any reason, or at any time upon request, I agree to return any and all patient confidential information in my possession. This is not a contract for continued employment.

I have read and understand all privacy policies and procedures that have been provided to me by The Westerville Division of Fire. I agree to abide by all policies or be subject to disciplinary action, which may include verbal or written warning, suspension, or termination of employment or of any membership or association with The Westerville Division of Fire. This is not a contract of employment and does not alter the nature of the existing relationship between The Westerville Division of Fire and me.

Signature: _____ *Date:*_____ *Printed*

Name:_____

The Westerville Division of Fire
Password Authorization Form

Name: _____ Date: _____

Address: _____

City: _____ State: _____ Zip Code: _____

Employee ID: _____

New Password ☐ Replacement Password ☐

Organizational Software _____

Mobil EMS Software _____

Employee Sign-on _____

Password _____

I agree that I will comply with all confidentiality policies and procedures set in place by The Westerville Division of Fire during my entire employment or association with The Westerville Division of Fire. If I, at any time, knowingly or inadvertently breach the patient confidentiality policies and procedure, I agree to notify the Privacy Officer of The Westerville Division of Fire immediately. In addition, I understand that a breach of patient confidentiality may result in suspension or termination of my employment or position at The Westerville Division of Fire. Upon termination of my employment or association with The Westerville Division of Fire for any reason, or at any time upon request, I agree to return any and all patient confidential information in my possession. This agreement is not a contract for continued employment.

Employee Signature _____

Privacy Officer Signature _____

Date _____

The Westerville Division of Fire
Policy on Security, Levels of Access and Limiting Disclosure and Use of PHI

Purpose

To outline levels of access to Protected Health Information (PHI) of various staff members of The Westerville Division of Fire and to provide a policy and procedure on limiting access, disclosure, and use of PHI. Security of PHI is everyone's responsibility.

Policy

The Westerville Division of Fire 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.

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
Billing Clerk	Intake forms from dispatch, patient care reports, billing claim forms, remittance advice statements, other patient records from facilities	May access only as part of completion of a patient event and post-event activities and only while actually on duty
Secretary	Intake forms from dispatch, patient care reports, billing claim forms, remittance advice statements, other patient records from facilities	May access only as part of duties to complete data entry and only during actual work shift

Lt./ Supervisor	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
Training Coordinator	Intake forms from dispatch, patient care reports	May access only as a part of training and quality assurance activities. All individually identifiable patient information should be redacted prior to use in training and quality assurance activities
Battalion Chief/ Deputy Chief/ Chief		May access only to the extent necessary to monitor compliance and to accomplish appropriate supervision and management of personnel

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 provided for in this and other policies and procedures and the justification for use of the entire medical record is specifically identified and documented.

Disclosures to and Authorizations From the Patient

You are not required to limit to the minimum amount of information necessary required to perform your job function, or your disclosures of PHI to patients who are the subject of the 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.

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 in non-recurring or non-routine, like making a request for documents via a subpoena, we must review make sure our request 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 need 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.

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.

Apparatus Areas: Staff members should be sensitive to that fact that members of the public and other agencies may be present in the apparatus area 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. See the The Westerville Division of Fire Policy on Use of Computer Equipment and Information Systems.

The Westerville Division of Fire
Policy on Use of Computer and Information Systems and Equipment

Purpose

The Westerville Division of Fire is committed to protecting our staff members, the patients we serve and the Department from illegal or damaging actions by individuals and the improper release of protected health information and other confidential or proprietary information.

The purpose of this policy is to outline the acceptable use of computer equipment at The Westerville Division of Fire. These rules are in place to protect the employee and patients of The Westerville Division of Fire. Inappropriate use exposes The Westerville Division of Fire to risks including virus attacks, compromise of network systems and services, breach of patient confidentiality and other legal claims.

Scope

This policy applies to employees, volunteers, contractors, consultants, temporary employees, students, and others at The Westerville Division of Fire who have access to computer equipment, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by The Westerville Division of Fire.

Procedure
Use and Ownership of Computer Equipment

1. All data created or recorded using any computer equipment owned, controlled or used for the benefit of The Westerville Division of Fire is at all times the property of The Westerville Division of Fire. Because of the need to protect the The Westerville Division of Fire computer network, the Department cannot guarantee the confidentiality of information stored on any network device belonging to The Westerville Division of Fire, except that it will take all steps necessary to secure the privacy of all protected health information in accordance with all applicable laws.

2. Staff members are responsible for exercising good judgment regarding the reasonableness of personal use and must follow operational guidelines for personal use of Internet/Intranet/Extranet systems and any computer equipment.

3. At no time may any pornographic or sexually offensive materials be viewed, downloaded, saved, or forwarded using any Department computer equipment. Please refer to the Department's Policy on Preventing Sexual and Other Harassment for further information.

4. For security and network maintenance purposes, authorized individuals within The Westerville Division of Fire may monitor equipment, systems and network traffic at any time, to ensure compliance with all Department policies.

Security and Proprietary Information

1. Confidential information should be protected at all times, regardless of the medium by which it is stored. Examples of confidential information include but are not limited to: individually identifiable health information concerning patients, Department financial and business information, patient lists and reports, and research data. Staff members should take all necessary steps to prevent unauthorized access to this information.

2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed regularly.

3. All PCs, laptops, workstations and remote devices should be secured with a password-protected screensaver, wherever possible, and set to deactivate after being left unattended for 10 minutes or more, or by logging-off when the equipment will be unattended for an extended period.

4. All computer equipment used by staff, whether owned by the individual staff member or The Westerville Division of Fire, shall regularly run approved virus-scanning software with a current virus database in accordance with Department policy.

5. Staff members must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses.

Unacceptable Use

Under no circumstances is a staff member of The Westerville Division of Fire authorized to engage in any activity that is illegal under local, state, or federal law while utilizing The Westerville Division of Fire computer resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities that fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or Department protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other

software products that are not appropriately licensed for use by The Westerville Division of Fire.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which The Westerville Division of Fire or the end user does not have an active license is strictly prohibited.

3. Exporting system or other computer software is strictly prohibited and may only be done with express permission of management.

4. Introduction of malicious programs into the network or server (e.g., viruses, worms, etc.).

5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

6. Using a The Westerville Division of Fire computer device to actively engage in procuring or transmitting material that is in violation of the Department's prohibition on sexual and other harassment.

7. Making fraudulent statements or transmitting fraudulent information when dealing with patient or billing information and documentation, accounts or other patient information, including the facsimile or electronic transmission of patient care reports and billing reports and claims.

8. Causing security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the staff member is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties.

9. Providing information about, or lists of, The Westerville Division of Fire staff members or patients to parties outside The Westerville Division of Fire.

E-mail and Communications Activities

1. Sending unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (e-mail Spam).

2. Any form of harassment via e-mail, telephone or paging, whether through language, frequency, or size of messages.

3. Unauthorized use, or forging, of e-mail header information.

4. Solicitation of e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies.

5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

6. Use of unsolicited e-mail originating from within The Westerville Division of Fire's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by The Westerville Division of Fire or connected via The Westerville Division of Fire's network.

Use of Remote Devices

The appropriate use of Laptop Computers, Personal Digital Assistants (PDAs), and remote data entry devices is of utmost concern to The Westerville Division of Fire. 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 Department information and these devices can be easily misplaced, lost, stolen or accessed by unauthorized individuals

1. Remote devices will not be purchased or used without prior Department approval.

2. The Department must approve the installation and use of any software used on the remote device.

3. Remote devices containing confidential or patient information must not be left unattended.

4. If confidential or patient information is stored on a remote device, access controls must be employed to protect improper access. This includes, where possible, the use of passwords and other security mechanisms.

5. Remote devices should be configured to automatically power off following a maximum of 10 minutes of inactivity.

6. Remote device users will not permit anyone else, including but not limited to user's family and/or associates, patients, patient families, or unauthorized staff members, to use Department-owned remote devices for any purpose.

7. Remote device users will not install any software onto any PDA owned by The Westerville Division of Fire except as authorized by the Department.

8. Users of Department-owned remote devices will immediately report the loss of a remote device to a supervisor and the Privacy Officer.

Enforcement

Any staff members found to have violated this policy may be subject to disciplinary action, up to and including suspension and termination.

The Westerville Division of Fire
Authorization to Use and Disclose
Specific Protected Health Information

By signing this Authorization, I hereby direct the use or disclosure by The Westerville Division of Fire 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 The Westerville Division of Fire and may be disclosed to:

_____
_____

I understand that I have the right to revoke this Authorization at any time except to the extent that The Westerville Division of Fire has already acted in reliance on the Authorization. To revoke this Authorization, I understand that I must do so by written request to The Westerville Division of Fire Privacy Officer [Deputy Chief Bernie Ingles 400 W. Main St. Westerville, Ohio 43081 (614) 901-6600].

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

I understand that my written authorization is not required for The Westerville Division of Fire 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 The Westerville Division of Fire for the following purpose(s):

_____
_____

The use or disclosure of the requested information will ___/will not ___ result in direct or indirect remuneration to The Westerville Division of Fire 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]

This authorization expires on: _____ (date or event).

The Westerville Division of Fire
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 Privacy Officer of The Westerville Division of Fire 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 Privacy Officer at the following address and phone number:

Deputy Chief Ingles
400 W. Main St.
Westerville, Ohio 43081
614-901-6600

YOU MAY ALSO MAKE A COMPLAINT TO THE GOVERNMENT

If you believe The Westerville Division of Fire is not complying with the applicable requirements of the Federal Privacy Rule you may file a complaint with the Secretary of the U.S. Department of Health and Human Services. 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.

(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, unless the Secretary for good cause shown waives this time limitation.

(4) 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.

(c) *Investigation.* The Secretary 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.

The Westerville Division of Fire
Log for Processing Complaints About Privacy Practices

DATE COMPLAINT RECEIVED	PATIENT NAME	DESCRIPTION OF COMPLAINT	DISPOSITION OF COMPLAINT

JOB DESCRIPTION

JOB TITLE: Privacy Officer

JOB IDENTIFICATION

Department: Fire Administration
Reports to: Fire Chief

JOB PURPOSE AND SUMMARY

The Privacy Officer oversees all activities related to the development, implementation, and maintenance of The Westerville Division of Fire'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).

This individual 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.

DUTIES AND RESPONSIBILITIES

Principle Responsibilities

1. Develop policies and procedures on staff training related to the privacy of patient health information and protected health information;

2. Develop policies on the security of health care information including computer and password security and patient data integrity;

3. Defines levels of staff access to PHI and minimum necessary requirement for staff based on the required job responsibilities;

4. Oversees, directs, delivers, and ensures the delivery of initial and ongoing privacy training and orientation to all staff members, employees, volunteers, students and trainees.

5. Serves as the contact person for the dissemination of PHI to other health care providers;

6. Serves as the contact person for patient complaints and requests;

7. Processes patient requests for access to and amendment of health information and consent forms;

8. Processes all patient accounting requests;

9. Ensures the capture and storage of patient PHI for the minimum period required by law;

10. Ensures ambulance service compliance with all applicable Privacy Rule requirements and works with legal counsel and other managers to ensure the Department maintains appropriate privacy and confidentiality notices and forms and materials.

11. Cooperates with the state and federal government agencies charged with compliance reviews, audits and investigations.

QUALIFICATIONS:

Educational Requirements

High school Diploma or GED Equivalent. Four-year college degree preferred, with a working knowledge of the Privacy Rule required.

Maintains current knowledge of applicable federal and state privacy laws and monitors changes in privacy practices for the ambulance industry to ensure current organizational compliance.

Mental Requirements of the Job

Reading and writing skills required. Experience working with the public is essential.

Demonstrated organizational, facilitation, communication and presentation skills.

Disclaimer

The information provided in this description has been designed to indicate the general nature and level of work performed by incumbents within this job. It is not designed to be interpreted, as a comprehensive inventory of all duties, responsibilities, qualifications and working conditions required of employees, assigned to this job. Management has sole discretion to add or modify duties of the job and to designate other functions as essential at any time. This job description is not an employment agreement or contract.

The Westerville Division of Fire
Job Description Language for Compliance with Privacy Practices

The following is recommended language to insert into all job or position descriptions within The Westerville Division of Fire to ensure that there is a strong focus on the protection of patient privacy in accordance with the Privacy Rule. It is recommended to add a subsection to the "duties and responsibilities" section of the position description specifically related to privacy issues:

Job Responsibilities Related to Patient Privacy

1. The incumbent is expected to protect the privacy of all patient information in accordance with the Department's privacy policies, procedures, and practices, as required by federal [and state] law, and in accordance with general principles of professionalism as a health care provider. Failure to comply with the Department's policies and procedures on patient privacy may result in disciplinary action up to and including termination of employment or of membership or association with The Westerville Division of Fire.

2. The incumbent may access protected health information and other patient information only to the extent that is necessary to complete your job duties. The incumbent may only share such information with those who have a need to know specific patient information you have in your possession to complete their job responsibilities related to treatment, payment or other Department operations.

3. The incumbent is encouraged and expected to report, without the threat of retaliation, any concerns regarding the Department's policies and procedures on patient privacy and any observed practices in violation of that policy to the designated Privacy Officer.

4. The incumbent is expected to actively participate in Department privacy training and is required to communicate privacy policy information to coworkers, students, patients and others in accordance with Department policy.

Disclaimer

The information provided in this description has been designed to indicate the general nature and level of work performed by incumbents within this job. It is not designed to be interpreted, as a comprehensive inventory of all duties, responsibilities, qualifications and working conditions required of employees, assigned to this job. Management has sole discretion to add or modify duties of the job and to designate other functions as essential at any time. This job description is not an employment agreement or contract.

The Westerville Division of Fire
Policy on Privacy Training

Purpose

To ensure that all members of The Westerville Division of Fire; including all employees, 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 the Department's policies and procedures regarding Protected Health Information (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.

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 the Department's policies and procedures on privacy practices.

Procedure

1. The Privacy Officer or his or her designee will conduct the Privacy Training.

2. All attendees will receive copies of the Department's policies and procedures regarding privacy.

3. All attendees must attend the training in person and verify attendance and agreement to adhere to the Department's policies and procedures on privacy practices.

4. The privacy officer will conduct the Mandatory Training in the following manner: A Microsoft PowerPoint presentation designed to comply with the Department's policies and procedures regarding privacy will identify key components of the program. Handouts will be provided for each of the necessary forms and the members will be trained in completion of the forms.

5. Topics of the training will include a complete review of the Department'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 the Department's specific privacy forms

The Westerville Division of Fire
Privacy Training Record Form

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

Date of Training: _____

Time Training Began:_____

Time Training Ended:_____

Training Location: _____

Trainer/Privacy Officer: _____

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 The Westerville Division of Fire and Procedures on Privacy Practices, a copy of which I received as part of the training materials for this session:

Date	EMS #	Name (Please Print)	Job Title	Signature Verification of Attendance

- Attach a copy of the program handouts and materials and keep in the Privacy Training file with this form for a minimum of six years from the date of initial training.

The Westerville Division of Fire
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 Privacy Officer, who oversees the Department's privacy compliance issues:

PRIVACY OFFICER

Name	Deputy Chief Ingles
Title	Deputy Chief
Address	400 W. Main St.
Phone Number	614-901-6600

TO FILE AN INTERNAL OR EXTENAL COMPLAINT ABOUT PRIVACY RELATED ISSUES, CONTACT:

Name	Deputy Chief Ingles
Title	Deputy Chief
Address	400 W. Main St.
Phone Number	614-901-6600

FOR QUESTIONS ABOUT DENIAL OF ACCESS TO PROTECTED HEALTH INFORMATION, CONTACT:

Name	Deputy Chief Ingles
Title	Deputy Chief
Address	400 W. Main St.
Phone Number	614-901-6600

FOR QUESTIONS ABOUT RECEIVING AND PROCESSING REQUESTS FOR ACCESS OR AMENDMENT TO PROTECTED HEALTH INFORMATION, CONTACT:

Name	Deputy Chief Ingles
Title	Deputy Chief
Address	400 W. Main St.
Phone Number	614-901-6600

ALTERNATE TO THE PRIMARY PRIVACY OFFICER

Name	Terry Smith
Title	EMS Coordinator
Address	400 W. Main St.
Phone Number	614-901-6600

The Westerville Division of Fire
Policy on Medical Records of Employees

Policy:

To provide guidance to management and staff concerning the privacy of medical records that involves staff members of The Westerville Division of Fire.

Procedure:

The Westerville Division of Fire 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 only have access to as much information as is minimally necessary for the legitimate use of the medical records.

In accordance laws concerning disability discrimination, all medical records of staff 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 Privacy Rule of the Health Insurance Portability and Accountabilities Act, 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 <u>not</u> considered to be protected health information, or 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 my 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.

Nonetheless, despite the fact that such records are not considered HIPAA protected, The Westerville Division of Fire will limit the use and disclosure of these records to only those with a need to have access to them, such as certain management staff, the Department's designated physician, and state agencies pursuant to state law.

With respect to staff members of The Westerville Division of Fire, only health information that is obtained about staff in the course of providing ambulance or other medical services directly to them is considered PHI under HIPAA. In other words, if The Westerville Division of Fire provides ambulance service to an employee, the protections typically given to such information to our ambulance service patients applies to the employee. These protections are subject to HIPAA exceptions, such as in the situation in

which the staff member used The Westerville Division of Fire involved in a work-related injury while on duty.

As another example, if we receive a staff member's medical record in the course of providing the employee with treatment and/or transport, it does not matter that The Westerville Division of Fire 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, The Westerville Division of Fire 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 The Westerville Division of Fire 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.

If you have any questions about how medical information about you is used and disclosed by The Westerville Division of Fire, please contact our Privacy Officer:

Deputy Chief Ingles
400 W. Main St.
614-901-6600

The Westerville Division of Fire
Sample Business Associate Contract Language
Billing Department

1. BILLING DEPARTMENT shall carry out its obligations under this Agreement in compliance with the privacy regulations pursuant to Public Law 104-191 of August 21, 1996, known as the Health Insurance Portability and Accountability Act of 1996, Subtitle F – Administrative Simplification, Sections 261, *et seq*., as amended ("HIPAA"), to protect the privacy of any personally identifiable protected health information ("PHI") that is collected, processed or learned as a result of the Billing Services provided hereunder. In conformity therewith, BILLING DEPARTMENT agrees that it will:

a. Not use or further disclose PHI except as permitted under this Agreement or required by law;

b. Use appropriate safeguards to prevent use or disclosure of PHI except as permitted by this Agreement;

c. To mitigate, to the extent practicable, any harmful affect that is known to BILLING DEPARTMENT of a use or disclosure of PHI by the BILLING DEPARTMENT in violation of this Agreement.

d. Report to The Westerville Division of Fire any use or disclosure of PHI not provided for by this Agreement of which BILLING DEPARTMENT becomes aware;

e. Ensure that any agents or subcontractors to whom BILLING DEPARTMENT provides PHI, or who have access to PHI, agree to the same restrictions and conditions that apply to BILLING DEPARTMENT with respect to such PHI;

f. Make PHI available to The Westerville Division of Fire and to the individual who has a right of access as required under HIPAA within 30 days of the request by The Westerville Division of Fire on the individual;

g. Incorporate any amendments to PHI when notified to do so by The Westerville Division of Fire;

h. Provide an accounting of all uses or disclosures of PHI made by BILLING DEPARTMENT as required under the HIPAA privacy rule within 60 days;

i. Make its internal practices, books and records relating to the use and disclosure of PHI available to the Secretary of the Department of Health and Human Services for purposes of determining BILLING DEPARTMENT'S and The Westerville Division of Fire’s compliance with HIPAA; and

j. At the termination of this Agreement, return or destroy all PHI received from, or created or received by BILLING DEPARTMENT on behalf of The Westerville Division of Fire, and if return is infeasible, the protections of this agreement will extend to such PHI.

2. The specific uses and disclosures of PHI that may be made by BILLING DEPARTMENT on behalf of The Westerville Division of Fire include:

a. The preparation of invoices to patients, carriers, insurers and others responsible for payment or reimbursement of the services provided by The Westerville Division of Fire to its patients;

b. Preparation of reminder notices and documents pertaining to collections of overdue accounts;

c. The submission of supporting documentation to carriers, insurers and other payers to substantiate the health care services provided by The Westerville Division of Fire to its patients or to appeal denials of payment for same.

d. Uses required for the proper management of the BILLING DEPARTMENT as a business associate.

e. Other uses or disclosures of PHI as permitted by HIPAA privacy rule.

3. Notwithstanding any other provisions of this Agreement, this Agreement may be terminated by The Westerville Division of Fire, in its sole discretion, if The Westerville Division of Fire determines that BILLING DEPARTMENT has violated a term or provision of this Agreement pertaining to The Westerville Division of Fire obligations under the HIPAA privacy rule, or if BILLING DEPARTMENT engages in conduct which would, if committed by The Westerville Division of Fire, would result in a violation of the HIPAA privacy rule by The Westerville Division of Fire.

NOTE: This is not a sample of a complete contract; only the HIPAA business associate provisions are provided.

The Westerville Division of Fire
Sample Business Associate Contract Language
Bricker & Eckler LLP

1. BRICKER & ECKLER LLP shall carry out its obligations under this Agreement in compliance with the privacy regulations pursuant to Public Law 104-191 of August 21, 1996, known as the Health Insurance Portability and Accountability Act of 1996, Subtitle F – Administrative Simplification, Sections 261, *et seq*., as amended ("HIPAA"), to protect the privacy of any personally identifiable protected health information ("PHI") that is collected, processed or learned as a result of the legal services provided to The Westerville Division of Fire by BRICKER & ECKLER LLP. In conformity therewith, BRICKER & ECKLER LLP agrees that it will:

a. Not use or further disclose PHI except as permitted under this Agreement or required by law;

b. Use appropriate safeguards to prevent use or disclosure of PHI except as permitted by this Agreement;

c. To mitigate, to the extent practicable, any harmful effect that is known to BRICKER & ECKLER LLP of a use or disclosure of PHI by the BRICKER & ECKLER LLP in violation of this Agreement.

d. Report to The Westerville Division of Fire any use or disclosure of PHI not provided for by this Agreement of which BRICKER & ECKLER LLP becomes aware;

e. Ensure that any agents or subcontractors to whom BRICKER & ECKLER LLP provides PHI, or who have access to PHI, such as consulting companies or other Bricker & Eckler LLPs, agree to the same restrictions and conditions that apply to BRICKER & ECKLER LLP with respect to such PHI;

f. Make PHI available to The Westerville Division of Fire and to the individual who has a right of access as required under HIPAA;

g. Incorporate any amendments to PHI when notified to do so by The Westerville Division of Fire;

h. Provide an accounting of all uses or disclosures of PHI made by BRICKER & ECKLER LLP as required under the HIPAA privacy rule;

i. Make its internal practices, books and records relating to the use and disclosure of PHI available to the Secretary of the Department of Health and Human Services for purposes of determining BRICKER & ECKLER LLP'S and The Westerville Division of Fire's compliance with HIPAA; and

j. At the termination of this Agreement, return or destroy all PHI received from, or created or received by BRICKER & ECKLER LLP on behalf of The Westerville Division of Fire.

2. The specific uses and disclosures of PHI that may be made by BRICKER & ECKLER LLP on behalf of The Westerville Division of Fire include, but are not limited to:

a. The review of patient care information in providing legal advice to The Westerville Division of Fire concerning a particular ambulance incident;
b. The review of patient care information and other medical records and the submission of that information to carriers, insurers and other payers with respect to BRICKER & ECKLER LLP assisting The Westerville Division of Fire in an insurance or Medicare audit or other similar action;
c. The review of patient care information with respect to providing The Westerville Division of Fire with legal advice generally;
d. The review of patient care information in the course of BRICKER & ECKLER LLP conducting compliance assessment activities;
e. The review of PHI and other information necessary to assist The Westerville Division of Fire in developing its HIPAA compliance program;
f. Other uses or disclosures of PHI as permitted by the HIPAA privacy rule.

3. Notwithstanding any other provisions of this Agreement, this Agreement may be terminated by The Westerville Division of Fire, in its sole discretion, if The Westerville Division of Fire determines that BRICKER & ECKLER LLP has violated a term or provision of this Agreement pertaining to The Westerville Division of Fire's obligations under the HIPAA privacy rule, or if BRICKER & ECKLER LLP engages in conduct which would, if committed by The Westerville Division of Fire, would result in a violation of the HIPAA privacy rule by The Westerville Division of Fire.

The Westerville Division of Fire
Confidentiality Agreement for Vendors Who Are Not Business Associates

CONFIDENTIALITY

1. CONTRACTOR understands that while performing the services under this contract, it will be working in areas where confidential and proprietary information may be kept, including confidential patient information. Under no circumstances, except as otherwise agreed to in writing, is any of the contractor's personnel to have access to any confidential information of The Westerville Division of Fire.

2. Further, in the event that CONTRACTOR inadvertently comes in contact with any confidential information, CONTRACTOR agrees not to use or further disclose such information to anyone.

3. CONTRACTOR further agrees to educate its personnel as to the importance of confidentiality with respect to the performance of this contract, and to maintain a strong confidentiality policy applicable to all of its personnel who may be assigned to perform services at The Westerville Division of Fire.

4. CONTRACTOR will take steps to ensure that its personnel remain only in authorized areas of The Westerville Division of Fire and that they will not open any files, desks, boxes, disk storage cases, or any other containers that may potentially contain confidential and proprietary information.

4. Any violations of this confidentiality provision shall be cause for immediate termination of this contract, without notice.