Waterford Fire and Rescue Department
Standard Operating Guidelines

ORIG. EFFECTIVE DATE	LAST REVISION	PAGES
4-14-2003	01-24-2014	
HIPAA SOG #	**SECTION**	**GUIDELINE**

TABLE OF CONTENTS

I. SAFEGUARDS

In accordance with the Health Insurance Portability and Accountability Act of 1996 and its amendments (HIPAA) and Wisconsin laws (referred to collectively as HIPAA or the Privacy Rule), the Village must have safeguards in place to protect the confidentiality, integrity and availability of all electronic and other protected health information (PHI) the Village creates, receives, maintains and transmits. The Village must protect against reasonably anticipated threats or hazards to the security and integrity of the information. It must also protect against reasonably anticipated uses or disclosures that are not permitted or required under law.

This document is created to ensure compliance with the law by the workforce of the Village of Waterford. Because PHI is initially created and kept by the members of the Waterford Fire and Rescue Department as part of the Village's rescue operations, much of this document is addressed to the members of the Department and is part of the Department's Standard Operating Guidelines (SOGs). Other Village staff is also involved in using PHI as part of payment and security operations, and these SOGs also apply to that staff insofar as they have access to and use PHI, and staff outside of the Department are required to acknowledge and agree to these provisions.

II. VERIFICATION OF CONFIDENTIALITY

The Waterford Fire and Rescue Department and Village staff have a legal and ethical duty to protect the privacy of all patients and the confidentiality of their health information. As a result, the Village has policies in place to assure the confidentiality of information. Given the nature of our work, it is imperative that we maintain the confidentiality of patient information that we receive in the course of our work. The Village prohibits the release of any patient information to anyone outside of the Department and certain Village staff unless required for purposes of treatment, payment, or health care operations, or as authorized by the patient or required by law, and discussions of Protected Health Information (PHI) within the Department and Village offices must be limited. Acceptable uses of PHI within the Village 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 Waterford Fire and Rescue Department provides services to patients that are private and confidential and that I am a crucial step in respecting the privacy rights of the Department's patients. I understand that it is necessary, in the rendering of the Department's 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 and privacy policies and procedures set in place by the Village of Waterford. If I, at any time, knowingly or inadvertently breach the patient confidentiality policies and procedures, or I am aware that another person has done so, I agree to notify the Privacy Officer immediately. In addition, I understand that a breach of patient confidentiality may result in suspension or termination of my employment or association with the Village. Upon termination of my employment or association for any reason, or at any time upon request, I agree to return any and all confidential patient information in my possession. This is not a contract for continued employment.

I agree not to discuss or to disclose any confidential information including any patient information, including patient name, outside of the Waterford Fire and Rescue Department or with authorized Village staff unless authorized to do so under this Policy or by law. I agree not to talk about confidential information in public places where others can overhear the conversation unless it is absolutely necessary under the circumstances.

I have read and understand all privacy policies and procedures that have been provided to me by the Village of Waterford, and have discussed any questions I have regarding this document with the Privacy Officer. I agree to abide by all policies or be subject to disciplinary action, which may include verbal or written warning, suspension, or termination of any employment, membership or association with the Waterford Fire and Rescue Department and/or the Village of Waterford. This is not a contract of employment and does not alter the nature of the existing relationship between the Waterford Fire and Rescue Department or the Village of Waterford and me.

_____ _____

Signature of Member or Staff Date

_____

Printed Name

_____

Signature of Privacy Officer

This Confidentiality Statement shall be interpreted and enforced in accordance with State and Federal laws.

III. CONFIDENTIALITY AND DISSEMINATION OF PATIENT INFORMATION

A. Purpose. All of the policies and procedures set forth in this document are necessary to ensure the confidentiality, integrity and availability of all electronic and non-electronic protected health information created, received, maintained or transmitted by the Waterford Fire and Rescue Department and the Village of Waterford as required by the Privacy Rule.

B. Policy. It is the policy of the Department to abide by the following policies and procedures that will ensure patient privacy rights in accordance with HIPAA.

1. All persons with access to PHI will sign a confidentiality statement whenever the policy is amended, and new members and authorized staff will be trained in the Privacy Rule and sign the confidentiality statement as soon as possible after becoming a member or being granted access to PHI. No person may ride along on a rescue call unless that person has, at a minimum, reviewed the Department's Privacy Policies and Procedures and signed the Verification of Confidentiality.

2. Under the Policy any and all patient identity and patient health information that is received, observed, witnessed and overheard is considered confidential. Therefore this information will not be disclosed to anyone other than those entities that need the information for continued patient care, e.g., treating hospital or higher level EMTs assisting with care, unless otherwise permitted under the Privacy Rule.

3. If any person feels that he or she, or another person, has breached patient confidentiality, the member must report it to the Privacy Officer.

4. If any complaints are received regarding a breach or potential breach of confidentiality, whether from a patient, a family member, the community or from another Department or staff member, the complaint will be referred to the Privacy Officer for review.

5. Depending upon the severity of the complaint the Privacy Officer may turn the complaint over to the Fire and Police Commission or the Village Board, as appropriate.

6. Depending upon the severity of the offense, the violator may receive a verbal or written warning, a suspension, or may be dismissed from the Department.

IV. SECURITY, LEVELS OF ACCESS AND LIMITING DISCLOSURE AND USE OF PHI

A. Purpose. To outline levels of access to Protected Health Information (PHI) of various members of the Waterford Fire and Rescue Department and authorized Village staff to provide a policy and procedure on limiting access, disclosure, and use of PHI. Security of PHI is everyone's responsibility.

B. Policy. The Village 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, and only to the extent that the person needs access to PHI to complete necessary job functions.

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

2. The Assistant Chief-EMS is the designated Privacy Officer, and shall have access to all PHI necessary to fulfill his or her duties. In the event that the Village of Waterford officially designates another person that may act for the Assistant Chief-EMS, that person shall also have the powers of the Privacy Officer.

C. 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.

1. Access to PHI is limited to the identified persons only, and to the identified PHI only, based on the Village’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.

2. 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.

Job Title	Description of PHI That May Be Accessed	Conditions of Access to PHI
EMT	WARDS, Street Sheet, Billing Sheet, RASO Run Time Reports, Medicare Information Sheets only for their own calls	May access only as part of completion of a patient event and post event activities, and only while actually on duty EMTs that are not members may not access WARDS, and must submit hard copies of patient care reports to the Waterford EMT
Assistant Chief-EMS/Privacy Officer and official designee	All PHI	May access as part of completion of a patient event and post event activities, duties related to patient billing and quality control and corrective counseling of staff, and as part of duties as Privacy Officer, and only while on duty
Staff and Business Associates responsible for billing;	WARDS, Billing Sheets, remittance advice statement, other patient records only as needed	May access only as part of duties to complete patient billing and follow-up and only during actual work shift
Firefighters, Trainees and Administrative Personnel	Street Sheets and Billing Sheets	May access only for obtaining and recording information from the patient or family members, and for recording other information given to them by the treating EMT(s), as directed by the EMT(s)
EMS Lieutenants	WARDS, Intake forms from dispatch, Street Sheets	May access only as a part of training and quality assurance activities. All individually identifiable patient information must be redacted prior to use in training and quality assurance activities
Fire Chief	PHI as needed for quality assurance	May access only the minimum necessary to monitor compliance and to accomplish appropriate supervision and management of personnel
Village Treasurer and Deputy Treasurer; Business Associate collection agencies and their attorneys; Village Administrator and Attorney	Street Sheets and Billing Sheets, remittance advice statement, other patient records only as needed	Minimum necessary to pursue unpaid bills, receive payments for services, process refunds and write-offs, and perform necessary accounting practices
Information Systems Personnel	Electronic PHI Supporting documentation	Only as necessary to perform system services, risk analysis and risk management duties
Medical Director	All PHI	As necessary for patient care and to perform quality assurance activities

D. Disclosures to and Authorizations from the Patient. Access to PHI is limited to the minimum amount of information necessary to perform a job function, and disclosures of PHI to patients who are the subject of the PHI is not limited. 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 or the Village.

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

2. As an example, if the Department has 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.

E. Department Requests for PHI. If the Department needs to request PHI from a health care provider or other entity, the request must be limited to only the reasonably necessary information needed for the intended purpose, as described below. For requests not covered below, the determination must be made individually for each request and the supervisor must be consulted for guidance. For example, if the request is non-recurring or non-routine, like making a request for documents via a subpoena, the Privacy Officer must review it and make sure the request covers only the minimum necessary PHI to accomplish the purpose of the request.

F. Report Procedure. It is the practice of the Waterford Fire and Rescue Department to secure all patient related material after delivering the patient to the treating hospital or returning from a rescue scene where a patient has refused transport.

1. After the treating EMTs return from the hospital or rescue scene, they will fill out the sign-in sheet, WARDS report, street sheet, billing sheet and Medicare paperwork when appropriate and retrieve the Racine County Sheriff's Office (RASO) Run Time Report. The EMT will enter the information in WARDS and sign out of WARDS as soon as the information is entered. An EMT that is not a member of the Department does not have access to WARDS, and is required to submit a patient care report in hard copy format to the Department EMT.

2. After all paperwork has been filled out the treating EMTs will place it into a secured locked container.

3. The Assistant Chief-EMS/Privacy Officer will take the paperwork from this secured locked container, review the information and the WARDS report, insert any needed information into the WARDS report, and secure the paperwork into the locked file cabinet.

4. The Assistant Chief-EMS/Privacy Officer and Fire Chief will have access to the files for Quality Control and for patients requesting access and/or amendments to their PHI.

5. The Village Attorney will have access to reports only as necessary to answer questions regarding the release or other handling of PHI.

6. Any report that is to be used for Quality Control / Assistance will have any and all Patient Identification blocked out to protect the patient's privacy.

V. PATIENT NOTIFICATION, ACCESS, AMENDMENT AND RESTRICTION ON USE OF PROTECTED HEALTH INFORMATION

A. Purpose. Under the Privacy Rule, individuals have the right to be notified of and have access to, and to request amendment to or restriction of the use of their PHI, and restrictions on its use that is maintained in "designated record sets," or DRS. (See Section VII, Designated Record Sets).

B. Policy. It is the policy of the Waterford Fire and Rescue Department to honor the patients' rights set forth in the HIPAA Privacy Rule.

1. To ensure that the Department properly notifies patients of their rights, and only releases the PHI that is covered under the Privacy Rule, this policy outlines procedures for notification of privacy practices, requests for patient access, amendment, and restriction on the use of PHI.

2. 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.

3. 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 Department.

C. Procedures.

1. Provision of the Notice of Privacy Practices.

a. Any person who requests a copy of the Notice of Privacy Practices will be provided with a copy upon request. The requestor does have to be a current patient.

b. In the event that the Department develops a website, the Notice of Privacy Practices will be posted on that site.

c. Every patient of the Waterford Fire and Rescue Department has the right to receive the Notice of Privacy Practices in a timely manner. The Notice will be provided whether or not the patient is transported. Whenever possible, the Notice will be provided on the date of treatment, as follows:

(1) The treating EMT will hand the patient the Notice of Privacy Practices and have the patient sign the Acknowledgement of Receipt of Notice of Privacy Practices as a record of receiving Notice. The Acknowledgement Form will be kept on file in the patient's Designated Record Set ("DRS" – see section VIII) in the Waterford Fire and Rescue Department files.

(2) If the patient is a minor the treating EMT will hand the Notice of Privacy Practices to the minor's parent or legal guardian. The minor patient's parent or legal guardian will be asked to sign the Acknowledgment Form as a record of receiving the Notice. A copy of the signed Acknowledgment will be kept in the patient's DRS in the Waterford Fire and Rescue Department files.

(3) If the patient is unresponsive or in a life threatening situation, or, in the judgment of the EMT, is too ill to acknowledge receipt of the Notice, or if the EMT is so involved with the emergency that it is not practical to provide the notice at the time of treatment, the treating EMT will fill out the Acknowledgement Form explaining the reason the Notice was not given to the patient at the time of treatment, and the manner in which the Notice will be provided to the patient. The Acknowledgement Form will be kept on file in the patient's DRS.

(4) If the treating EMT feels the patient has altered mental status the EMT will also send a copy of the Notice in the mail.

(5) If the patient requests the treating EMT to explain or read the Notice of Privacy Practices, the EMT will do so if time allows.

(6) Any personal health information (PHI) obtained by any member of the Department during the course of treatment of a patient will be used only for purpose of treatment, billing and health care operations, unless otherwise allowed under HIPAA.

(7) Any Firefighter that obtains PHI will do so for the sole purpose of assisting the EMT(s) in treatment of the patient. Any information obtained by the firefighter will be considered confidential.

(8) All DRS will be kept for no less than six years or as otherwise required by laws and regulations.

2. Access, Amendment and Restriction of Records.

a. Patient Access.

(1) A patient or appropriate representative may complete a Request for Access form at the Safety Building during regular business hours. The Privacy Officer will receive the request for access. If the Privacy Officer is unavailable the duty to receive the request will fall upon any available EMT.

(2) The person receiving the request for access must verify the patient's identity, and if the requestor is not the patient, the name of the individual and reason that the request is being made by this individual. The use of a driver's license or other form of government-issued identification is acceptable for this purpose. Requests received by mail will be evaluated pursuant to the separate Policy for Evaluation of PHI Requests Received from Third Parties.

(3) The Privacy Officer will evaluate the request. If the Privacy Officer has a question about the release of information, he or she will consult with the Waterford Village Attorney.

(4) The Privacy Officer will act upon the request as soon as possible. Generally, the Department must respond to requests for access to PHI within 30 days of receipt of the access request, unless the DRS 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 the required time frame, 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, the patient will have the right to access the PHI contained in the DRS outlined below and may make a copy of the PHI contained in the DRS upon verbal or written request. The patient and Privacy Officer will arrange a mutually convenient time for the patient to inspect and/or obtain a copy of the requested PHI. The inspection of the PHI will be done within the Safety Building with the assistance of the Privacy Officer. If the patient chooses to receive a copy of the PHI, the Privacy Officer will provide this service. The patient may request that this copy be mailed.

(7) If the Patient requests electronic copies of the PHI, and the information is available electronically, the Privacy Officer will provide the PHI electronically.

(8) The Department will charge reasonable cost based copying fees for the records, as authorized by Federal Law, in the same amounts set forth in the Fee Schedule for the Village of Waterford. If the cost of providing the PHI electronically is lower than that of standard copies, the lower cost shall be charged.

(9) 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.

(10) 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) The information the patient requested was compiled in reasonable anticipation of, or use in, a civil, criminal or administrative action or proceeding;

(b) 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.

(c) The person making the request for access is barred from such access by state or federal law.

(11) The following reasons to deny access to PHI are subject to review and the patient may appeal the denial:

(a) 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) 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) 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 is reasonably likely to cause harm to the individual or another person;

(12) If the denial of the request for access to PHI is for reasons (11) (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. 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.

(13) If the patient is dissatisfied with the response of the Department, 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.

(14) Access to the actual files or computers that contain the DRS of the patient is not 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 the Privacy Officer. UNDER NO CIRCUMSTANCES WILL ORIGINALS OF PHI LEAVE THE PREMISES.

(15) Whenever a patient or requestor is allowed access to or provided copies from a DRS, a note will 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 given to the patient or requestor.

(16) Following a request for access to PHI, a patient or requestor may request an amendment to the PHI, and request restriction on its use in some circumstances.

b. Requests for Amendment to PHI.

(1) If upon inspection of the PHI the patient feels it is inaccurate or incomplete, the patient has the right to request an amendment to the PHI. The patient or appropriate requestor may only request amendment to PHI contained in the DRS. The "Request for Amendment of PHI" Form must accompany any request for amendment. The Department may grant the request unless:

(a) The originator of the record is no longer available.

(b) The information the patient is requesting to amend was not created by the Department. The information is not part of the patient care record.

(c) The information is accurate and complete.

(d) The information would not be available for inspection as provided by law, and therefore the Department is not required to consider an amendment. (This exception applies to information compiled in anticipation of a legal proceeding.)

(e) The information was received from someone else under a promise of confidentiality.

(2) Procedure.

(a) Confirm the identity of requestor or legal representative. If the requestor is a legal representative, ask for legal proof of their representative status.

(b) The patient must fill out the Request for Amendment of Health Information form completely. 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.

(c) The Department, with the assistance of legal counsel, will act on the request for amendment within 60 days of the request.

(d) All requests for amendment must be forwarded immediately to the Privacy Officer for review.

(e) 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.

(3) Granting Requests for Amendment.

(a) If the Privacy Officer grants the request for amendment, then the Privacy Officer will amend the PHI and will send a letter indicating that the appropriate amendment to the PHI or record that was the subject of the request has been made.

(b) The Privacy Officer must provide the amended information to those individuals identified by having received the PHI that it has been amended, as well as to 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.

(4) Denial of Requests for Amendment.

(a) The Department may deny a request to amend PHI for any of the reasons stated in (1)(b) above.

(b) The Privacy Officer must provide a written denial, and include the following information:

[1] The person may submit a short written statement disagreeing with the denial, and how the individual may file such a statement.

[2] The person may, if he or she does not wish to submit a statement of disagreement, may request that the request for Amendment and the denial become a permanent part of their medical record.

[3] The person may complain to the Department Privacy Officer at 122 North Second Street, Waterford, WI 53185, or to the federal agency that oversees enforcement of the federal Privacy Rule, the Department of Health and Human Services.

[4] If the individual submits a "statement of disagreement," the Privacy Officer 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 Privacy Officer.

(5) All documentation pertaining to the request for amendment will be kept in the DRS.

(6) If the Department receives a notice from another covered entity, such as a hospital, that it has amended its PHI in relation to a particular patient, the Department must amend its own PHI that may be affected by the amendment.

c. Requests for Restriction.

(1) A patient may request a restriction on the use and disclosure of his or her PHI.

(a) The Department is not required to agree to most restrictions, and given the emergent nature of the Department operation, the Department generally will not agree to a restriction, except as set forth in subsection (b).

(**b) The Department must agree to a request to restrict disclosure of PHI to a health plan if the disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law; and the PHI pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the Department in full.**

IF A PATIENT TELLS THE EMT THAT HE OR SHE WILL PAY THE ENTIRETY OF THE BILL, THE EMT MUST PLACE A FLAG ON WARDS AS FOLLOWS: "PATIENT IS A SELF-PAY, DO NOT BILL INSURER."

(2) All requests for restriction on use and disclosure of PHI must be submitted in writing on the Request for Restriction form. All requests will be reviewed and denied or approved by the Privacy Officer.

(3) If the Department agrees to a restriction, PHI may not be used or disclosed 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.

(4) The agreement to restrict PHI will be documented to ensure that the restriction is followed.

(5) A restriction may be terminated if the individual agrees to or requests the termination. Oral agreements to terminate restrictions must be documented. A current restriction may also be terminated by the Department as long as the Department notifies the patient that PHI created or received after the restriction is removed is no longer restricted. PHI that was restricted prior to the Department voiding the restriction must continue to be treated as restricted PHI.

d. Evaluation of PHI Requests Received from Third Parties. Under the Privacy Rule, the Department, as a covered entity, may not reveal PHI for purposes other than treatment, payment, and health care operations unless the Department has the individual's authorization or is otherwise required by law to reveal the PHI. The Department will honor a patient's valid authorization to release PHI to third parties. In order to determine whether the authorization is valid, the Department will follow the procedure set forth herein. The Department will also respond to court orders and legal process, or make other disclosures required by law, as set forth herein.

(1) Written Authorization. When a written authorization for the release of PHI is received by the Privacy Officer, that authorization will be checked for the following core elements required by HIPAA:

(a) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.

(b) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.

(c) The name or other specific identification of the person(s), or class of persons, to whom the Department may make the requested use or disclosure.

(d) A description of each purpose of the requested use or disclosure. The statement "At the request of the

individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.

(e) An expiration date or expiration event that relates to the individual or the purpose of the use or disclosure. The statement "end of the research study," "none," or similar language is sufficient if the authorization is for a use or disclosure of PHI for research, including for the creation and maintenance of a research database or research repository.

(f) Signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of the representative's authority to act for the individual must also be provided.

(2) In addition to the core elements, the authorization must also be checked for the following statements (or similar wording), which must be adequate to place the individual on notice of all of the following:

(a) The individual's right to revoke the authorization in writing, and either:

[1] The exceptions to the right to revoke and a description of how the individual may revoke the authorization; or

[2] To the extent that the information in (2)[a] is included in the Waterford Fire and Rescue Department Notice of Privacy Practices, a reference to the Department's Notice.

(b) The ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization, by stating either:

[1] The covered entity may not condition treatment, payment, enrollment or eligibility for benefits on

whether the individual signs the authorization when a prohibition on conditioning of authorizations in HIPAA applies; or

[2] The consequences to the individual of a refusal to sign the authorization when, in accordance with HIPAA, the covered entity can condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain such authorization.

[3] The potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer be protected by this rule.

(3) If the authorization does not contain these elements, the authorization will be returned to the requestor with a statement of the deficiency. If the authorization includes these elements, only the specific information that is requested will be sent to the requestor. The Privacy Officer will send a bill for the information for the amount determined appropriate pursuant to the Fee Schedule of the Village of Waterford, or if sent electronically, for the reduced costs related to electronic transmission. If the Privacy Officer is not sure whether the authorization is sufficient, he or she will consult with the Village Attorney.

d. Judicial and Administrative Proceedings. The Department will disclose PHI in the course of administrative or judicial proceedings as follows:

(1) In response to an order of the court or administrative tribunal, the Department will disclose only the information expressly authorized by the order.

(2) In response to a subpoena, discovery request, or other lawful process that is not accompanied by an order of a court or administrative tribunal, the Department will disclose only the information expressly requested if:

(a) The Department receives satisfactory assurance from the party seeking the information that reasonable efforts have been made by the party to ensure that the individual who is the subject of the requested PHI has been given notice of the request; or

(b) The Department receives satisfactory assurance from the party seeking the information that reasonable efforts have been made by the party to secure a qualified protective order that meets the requirements of HIPAA.

(3) If a subpoena, discovery request or other lawful process does not contain the required satisfactory assurance, it will be referred to the Village Attorney.

(4) The Privacy Officer will send a bill for the information for the amount determined appropriate under the Fee Schedule of the Village of Waterford, or if sent electronically, for the reduced costs related to electronic transmission.

3. Other Uses and Disclosures Required by Law. The Department may make other uses and disclosures of PHI as set forth in the HIPAA law, including, but not limited to: for public health activities; when there is a reasonable belief that an individual is a victim of abuse, neglect, or domestic violence; for health oversight activities; for law enforcement purposes; about decedents; for research purposes; or to avert a serious threat to health or safety. All such disclosures will be made strictly pursuant to the HIPAA law.

4. Verification of Identity of Requestor. The Privacy Officer will verify the identity of the person requesting the PHI and the authority of the person to have access to the PHI if the person is not known to the Department. The Privacy Officer will also obtain any documentation, statements, or representations, whether oral or written, from the requestor when required by HIPAA. If the Privacy Officer, in his or her professional judgment, questions the identity or authority of the person making the request, he or she will refer the request to the Village Attorney.

5. Documentation. All requests for PHI under this policy will be logged in the patient's DRS and in the Department's Accounting Log. The original authorization or other legal process received will be kept in the patient's DRS, and a copy returned with the information disclosed. The disclosed information will conform to the "minimum necessary" rule as provided by HIPAA.

VI. DEPARTMENT PERSONNEL RESPONDING TO RESCUE/FIRE CALLS

Department personnel may respond to any Rescue/Fire call for which that person is available. Any patient information or PHI that member of the Department obtains, sees or hears is confidential and falls

under the HIPAA law. Any breach of confidentiality will be dealt with according to the SOGs and the Personnel Manual.

VII. DESIGNATED RECORD SETS

A. Purpose. To ensure that the Department releases Protected Health Information (PHI) in accordance with the Privacy Rule, this policy establishes a definition of what information should be included as part of the DRS. Under the Privacy Rule, the DRS includes medical records that are created or used by the Department to make decisions about the patient.

B. 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 information included in the DRS consists of medical records, billing records and payment records. Billing and Payment records may be kept off-site at the Village Hall and in the offices of Business Associates.

C. The Designated Record Set.

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

a. The Street Sheet created by Rescue personnel (this includes any photographs or monitor strips), Refusal of Care forms, the Run Time Report from RASO, acknowledgement of receipt of Notice of Privacy Practices, Medicare Assignment, Billing Sheet, and any other or other source data.

b. The electronic Wisconsin Ambulance Run Data System (WARDS) report, electronic claims records or other paper records of submission of actual claims to the billing company, 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 authorizations 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 includes 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.

3. The records related to payments made, including through the Village's billing and collection Business Associates, are part of the DRS but are kept in locked files in the office of the Village Treasurer.

IX. COMPUTER AND INFORMATION SYSTEMS AND EQUIPMENT

A. Purpose. The Village is committed to protecting Department members and staff, the patients served, 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 used for PHI. These rules are in place to protect the patients of the Waterford Fire and Rescue Department along with the Village as a whole. Inappropriate use exposes the Village to risks including virus attacks, compromise of network systems and services, breach of patient confidentiality and other legal claims.

B. Policy. This policy applies to employees, volunteers, contractors, consultants, temporary employees, students, and others at the Department and other Village offices 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 Village of Waterford.

C. Use of Computer Equipment.

1. The Village of Waterford policies regarding the Use of Electronic Information Systems, Electronic Information Systems Security, and Personal Use of Electronic Information Systems set forth in the Village of Waterford Personnel Manual are incorporated herein as though fully set forth, inclusive of the provisions for discipline for violation of those policies.

2. The Waterford Fire and Rescue Department and the Village of Waterford will take all steps necessary to secure the privacy of all protected health information in accordance with all applicable laws.

3. For security and network maintenance purposes, authorized individuals may monitor equipment, systems and network traffic at any time, to ensure compliance with all Village and Department policies.

4. Upon termination of any person's association with the Village, the Privacy Officer and/or the Village Administrator will terminate that person's ability to access the system.

D. Security and Proprietary Information. Confidential information must be protected at all times, regardless of the medium in which it is stored. Examples of confidential information include but are not limited to: individually identifiable health information concerning patients, patient lists and reports, and research data. Members and staff must take all necessary steps to prevent unauthorized access to this information.

1. Each person who is authorized to use and access PHI receives a unique password for access to Village computers, and another unique password for access to WARDS (if authorized), and is responsible for keeping passwords secure and for not sharing accounts. Authorized users are responsible for the security of their passwords and accounts.

2. No PHI shall be entered into devices owned by staff. Only Village issued devices may be used for entry of PHI. Village owned devices are protected by security software.

3. No person shall make fraudulent statements or transmit fraudulent information when dealing with patient or billing information and documentation, accounts or other patient information, including the facsimile or electronic transmission of PHI.

4. No person may alter or destroy PHI. If PHI must be amended, it will be done by the Privacy Officer, or under his or her direct supervision.

E. Use of Remote Devices. The appropriate use of laptop computers, smart phones, personal digital assistants (PDAs), and remote data entry devices is of utmost concern to the Village. 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 may not be used without prior Department approval. No unauthorized software may be installed on a Village owned remote device. No remote device not owned by the Village may be used for confidential or patient information.

2. If confidential or patient information is stored on a Village owned remote device, access controls must be employed to protect improper access. The device may not be left unattended.

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

4. Users of Village-owned remote devices must immediately report the loss or theft of a remote device to the Privacy Officer.

F. Risk Analysis; System Security.

1. The Village Administrator, Fire Chief, Privacy Officer, and Village Treasurer, along with the Village's Information Systems consultant, shall perform the Risk Analysis required under HIPAA set forth in 45 CFR s. 164.308 at least annually. The risk analysis shall include an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic PHI held by the Village. If the measures set forth in this document are insufficient, the Village shall implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. Documentation of the Risk Analysis shall be kept by the Privacy Officer.

2. The Privacy Officer will monitor access to the WARDS system by members of the Waterford Fire and Rescue Department, will post security reminders, and will provide periodic security updates as necessary.

3. The Village's contingency plan for continued operations, data backup plan, and emergency mode operation plan will apply to PHI.

4. When hard copies of PHI are disposed of pursuant to the established destruction schedules of the Village, those hard copies shall be securely shredded. When PHI is contained on electronic media and/or hardware, that media or hardware shall be physically destroyed to prevent unauthorized access to the PHI. Electronic media

and hard drives containing PHI shall not be reused or sold, provided however that a hard drive may be removed from a computer to enable recycling of the rest of the hardware.

G. Business Associates. Business Associates receiving PHI shall be subject to HIPAA, and the Village will reflect this requirement in all contracts entered into with Business Associates.

H. Enforcement. Any person found to have violated this policy will be subject to disciplinary action, up to and including suspension and termination. Revocation of system privileges (permanent or temporary), retraining, and other appropriate measures may be imposed.

X. PRIVACY TRAINING

A. Purpose. To ensure that all employees of the Village of Waterford and members of the Waterford Fire and Rescue Department—including all employees, volunteers, students and trainees (collectively referred to as "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).

B. Policy. All individuals who have access to PHI are required to undergo privacy training in accordance with the HIPAA Privacy Rule.

1. All new staff will be required to undergo privacy training in accordance with the Privacy Rule within a reasonable time upon association with the Department, as scheduled by the Privacy Officer.

2. All 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.

C. Procedure. The Privacy Training will be conducted by the Privacy Officer, or his or her designee.

1. All attendees will receive copies of the Village’s policies and procedures regarding privacy.

2. All attendees must attend the training in person, verify attendance, and sign an

agreement to adhere to the Department's policies and procedures on privacy practices.

3. Training will be conducted in the following manner: The members will view a training video and will receive a packet including all of the Village's privacy policies and procedures, which will be reviewed with them, and will participate in a question and answer session following both the viewing of the video and the review of the policies.

4. Topics of the training will include a complete review of the Department's Standard Operating Guideline on HIPAA 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 (H1PAA) and amendments thereto.

    b. Description of protected health information (PHI).

    c. Patient rights under the HIPAA Privacy Rule.

    d. Member and staff 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.

XI. FILING A COMPLAINT ABOUT PRIVACY PRACTICES

A. An Individual May Make a Complaint Directly to the Department. An individual has the right to make a complaint directly to the Privacy Officer of the Waterford Fire and Rescue Department concerning its policies and procedures with respect to the use and disclosure of protected health information (PHI). An individual may also make a complaint about concerns the person has regarding the Department's compliance with

any established policies and procedures concerning the confidentiality and use or disclosure of PHI, or about the requirements of the federal Privacy Rule.

All complaints should be directed to the Privacy Officer at the following address and phone number:

Privacy Officer
Waterford Fire and Rescue Department
122 North Second Street, Waterford, WI 53185
(262) 534-3911

B. An Individual May Make a Complaint to the Federal Government. If an individual believes the Village or the Waterford Fire and Rescue Department is not complying with the applicable requirements of the Federal Privacy Rule, the individual may file a complaint with the Secretary of the U.S. Department of Health and Human Services.

C. 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.

5. 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.